# Chameleon Pro

## Mode d'emploi du Dispositif Master






Table des matières

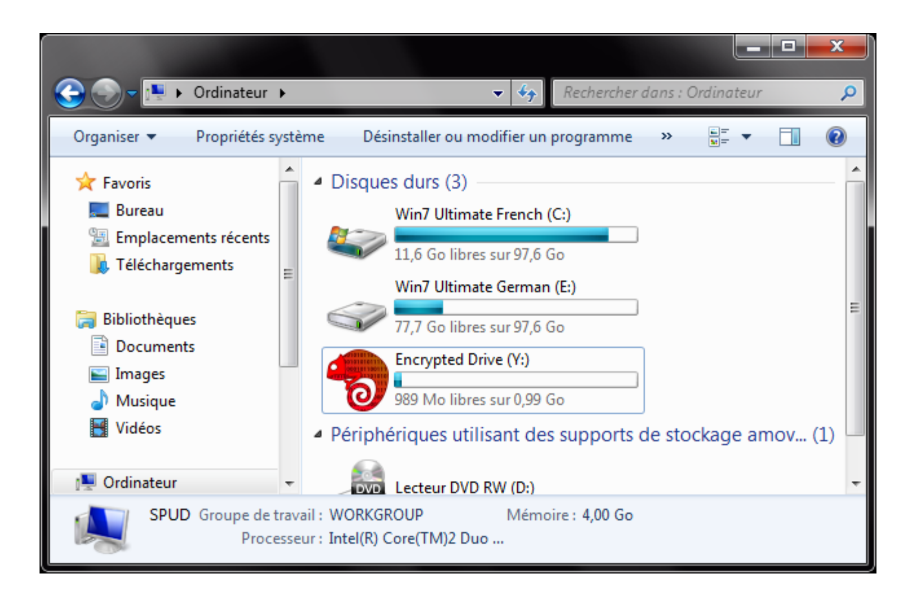




485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

# 1 Introduction

Le Chameleon Pro protège les fichiers de votre PC grâce à un cryptage AES-256. Contrairement aux autres dispositifs USB de cryptage, Chamelon Pro protège les fichiers sur le disque dur au lieu de les transférer vers un dispositif USB. Le Chameleon Pro créé un disque crypté en utilisant l'espace libre de votre disque dur. Les fichiers et applications enregistrés sur ce disque crypté sont protégés et on ne peut y avoir accès que lorsque le dispositif Chameleon est connecté. Tout comme votre clé de voiture, le dispositif agit en tant que clé matérielle pour votre disque dur.




Le Chameleon Pro inclut deux types de dispositifs : Masters et Utilisateurs. Les dispositifs Utilisateur fournissent toutes les fonctions Chameleon principales de sécurité (disques cryptés, cryptage de fichier individuel, etc.). Les dispositifs Master offrent les mêmes fonctions tout en permettant de gérer les Utilisateurs.

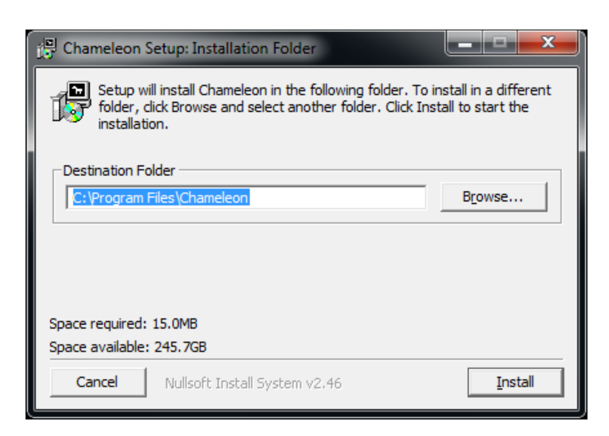
Un Master peut créer des Utilisateurs, y avoir accès, les dupliquer, paramétrer leurs termes, et les verrouiller. Alors que les Utilisateurs n'ont pas accès aux données protégées par d'autres Utilisateurs, le Master, lui, a accès aux données protégées par n'importe quel Utilisateur auquel il est associé. Un Master peut aussi gérer ses propres données cryptées indépendantes.

Le Chameleon Pro fonctionne sur les PC équipés de Windows XP, Vista et Win7.

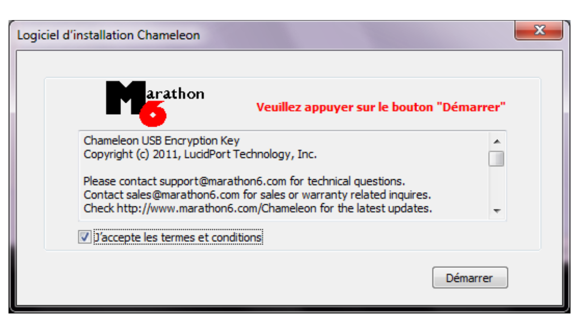
# 2 Installation du Master Chameleon Pro

1. Avant d'installer le logiciel Chameleon, vérifiez que toutes les versions précédentes du Chameleon soient bien désinstallées. La désinstallation ne supprime pas les disques cryptés existants.

2. **Insérez le CD d'installation** et **exécutez le programme Installation**.[1] (Vous pouvez également télécharger le programme d'installation ici : http://www.zepla.fr/telechargement.)
3. **Cliquez sur le bouton « Installer »** pour charger le logiciel.




4. **Insérer votre nouveau dispositif Master** puis **cliquez sur « Démarrer »** pour lancer l'assistant à l'installation, ceci afin de démarrer la configuration du Master. (Les dispositifs Utilisateurs seront configurés plus tard)




5. **Choisissez entre A), B), ou C)**




**A) Choisissez une phrase de passe de récupération**. Cette phrase de passe est utilisée uniquement pour créer des doubles de votre dispositif Master (au cas où vous le perdriez) et n'est pas utilisée en fonctionnement normal. Vous pouvez voir votre phrase de passe de récupération comme un mot de passe sauvegardé dans le dispositif lui-même.

Sélectionnez une phrase de passe unique. Il est possible qu'un autre Master ayant la même phrase de passe accède à vos données. Une fois programmée, la phrase de passe de récupération ne peut jamais être changée.

[1] Sur certains ordinateurs fonctionnant sous Windows7, il se peut que vous receviez un avertissement du Contrôle de Compte Utilisateur vous informant qu'un programme essaye d'effectuer des changements sur votre ordinateur. Dans ce cas, sélectionnez « Oui » ou « Installer ».





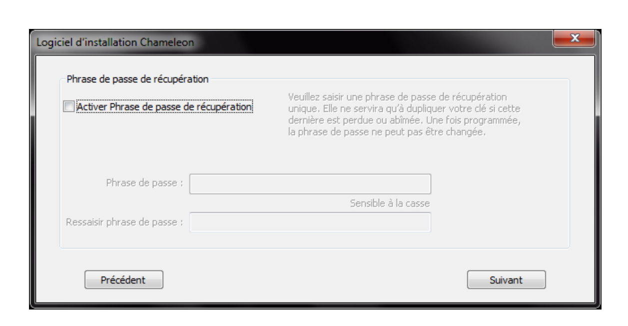


485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

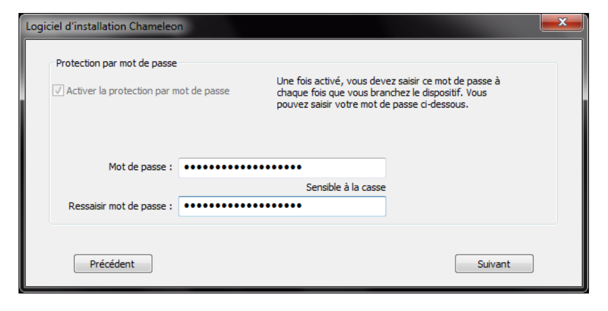
Pour être efficace, une phrase de passe devrait faire au moins 16  caractères de long (plus elle est longue, plus elle est sûre) et devrait inclure des lettres aléatoires (majuscules et minuscules), des chiffres et des symboles spéciaux.  Protégez votre phrase de passe comme vous protégeriez un mot de passe. Un assaillant qui prendrait connaissance de votre phrase de passe pourrait l'utiliser pour créer le double d'un dispositif Master. Il n'existe aucun moyen de dupliquer un dispositif Master sans votre phrase de passe de récupération.

**B)** Pour un équilibre optimal entre sécurité et redondance, utilisez une séquence aléatoire d'au moins 64 chiffres et lettres comme phrase de passe. Une fois l'installation terminée, créez plusieurs dispositifs Master avec cette séquence, comme copies de sauvegarde. (Voir « `5 Dupliquer un dispositif Master` »). Afin de pouvoir créer des doubles supplémentaires du Master à l'avenir, sauvegardez la séquence aléatoire dans un emplacement sûr. Sinon, supprimez la séquence.

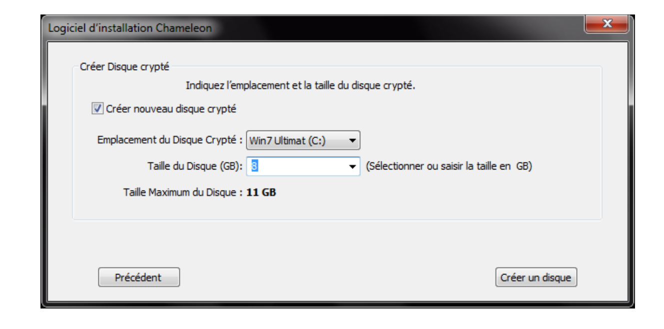
**C) Désactivez la phrase de passe de récupération.** Pour une sécurité maximum, désactivez la phrase de passe de récupération. Ceci donne l'ordre au dispositif de générer sa propre clé de cryptage aléatoire. Cela signifie cependant que vous ne pourrez pas dupliquer ou remplacer le dispositif s'il est perdu ou endommagé.




6. **Choisissez un mot de passe**. Les dispositifs Master sont toujours protégés par mot de passe. Les mots de passe ne sont pas facultatifs pour les Masters. (Les mots de passe sont facultatifs sur les dispositifs Utilisateur.) Le mot de passe doit être saisi à chaque fois que vous branchez l'appareil. Il doit être différent de la phrase de passe de récupération. Un mot de passe protège votre dispositif Master contre toute utilisation non autorisée.




7. **Créez un disque crypté.** Ce disque sera accessible uniquement par le dispositif Master. Un disque crypté appartenant au Master est obligatoire pour dupliquer ou remplacer des dispositifs Master.




Indiquez la taille et l'emplacement du disque. Le programme d'installation créé le disque crypté

en utilisant l’espace libre à cet emplacement. Le disque crypté n’a pas besoin d’être de grande taille. Il peut résider sur votre disque dur local ou sur des disques USB externes. Sa taille peut être modifiée ultérieurement en utilisant le logiciel Gestionnaire Chameleon (Démarrer > Tous les programmes > Chameleon > Gestionnaire Chameleon).

La totalité du contenu copié sur le disque crypté est protégée automatiquement. Elle est accessible lorsque le dispositif est inséré et disparaît lorsque le dispositif est retiré.

### *2.1 Désinstaller*

Vous pouvez désinstaller le logiciel Chameleon en localisant « Chameleon » à partir du menu Démarrer de Windows et en sélectionnant « Désinstaller » (Démarrer > Tous les programmes > Chameleon > Désinstaller). La désinstallation ne supprime pas vos disques cryptés. Afin de supprimer des disques cryptés, supprimez le répertoire ChameleonDrives à partir du répertoire de haut niveau de votre disque dur (par ex : C:\ ChameleonDrives\). Le répertoire ChameleonDrives ne peut être supprimé que lorsque le dispositif Chameleon n’est pas connecté.

## 3 Disques cryptés Chameleon : protéger vos données

Connectez votre dispositif  Chameleon pour accéder au disque crypté. Le disque crypté apparaît comme n’importe quel disque dur sur votre système. Vous pouvez y enregistrer des fichiers, y ouvrir des fichiers, y installer et exécuter des programmes, déplacer des fichiers d’un répertoire à l’autre et indiquer à des applications d’utiliser le disque crypté.  Une fois le dispositif Chameleon retiré, le disque crypté disparaît de Windows. Une analyse approfondie de votre disque dur ne révélerait que des données cryptées, d’apparence aléatoire.

Seuls les fichiers enregistrés sur le disque Chameleon sont cryptés. Tout fichier copié ou lu à partir du disque crypté est automatiquement décrypté. Par exemple, si un utilisateur joignait un fichier du disque crypté à un e-mail, ce fichier serait attaché décrypté.  Pour la sécurisation des pièces jointes dans les e-mails et du Cloud Storage, voir la rubrique « 7 Crypter des fichiers et dossiers individuels ».

Vous pouvez copier des fichiers sur le disque crypté en utilisant simplement la commande « glisser-déposer » pour les y déplacer. Cependant, le fichier original non crypté est conservé à son emplacement original. Un « glisser-déposer» effectué avec un clic droit est une méthode plus sécurisée. Maintenez le bouton droit de la souris appuyé, puis faites glisser le fichier sélectionné vers le disque crypté. Une boîte de dialogue apparaîtra alors indiquant « Copier », « Déplacer », et « Sécuriser déplacer ». L’option Sécuriser Déplacer déplace le fichier vers le disque crypté, puis élimine toute trace de ce fichier à son emplacement d’origine.[2] Cela peut prendre un certain temps s’il s’agit d’une quantité de données importante.

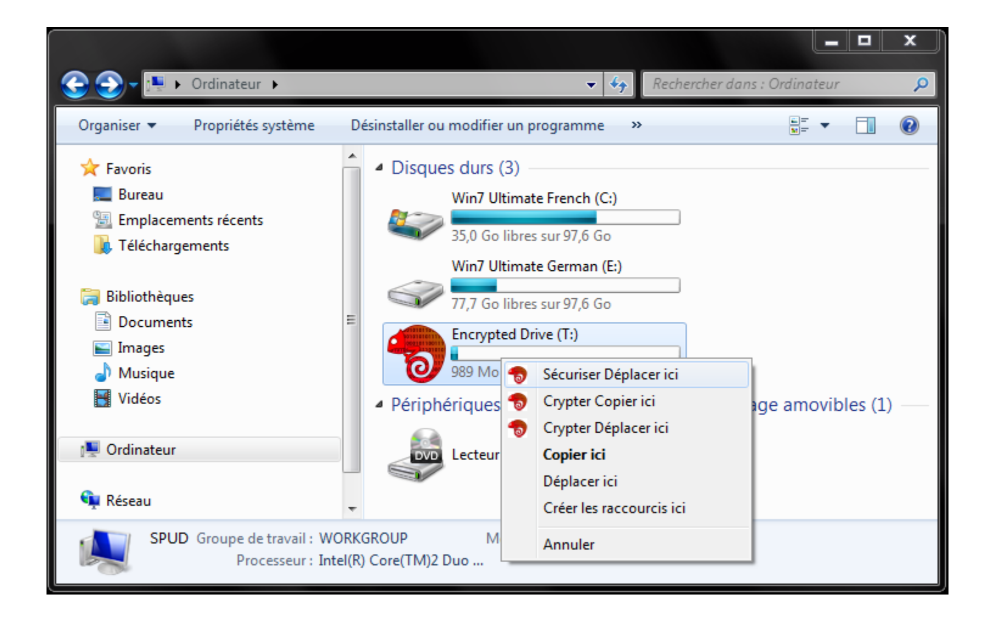
[2] La commande « Déplacer » standard de Windows copie le fichier, puis caractérise le fichier d’origine en tant que fichier supprimé. Il est possible de récupérer le fichier supprimé grâce à des outils spécialisés. L’option « Sécuriser Déplacer » empêche la récupération en écrasant le fichier supprimé.





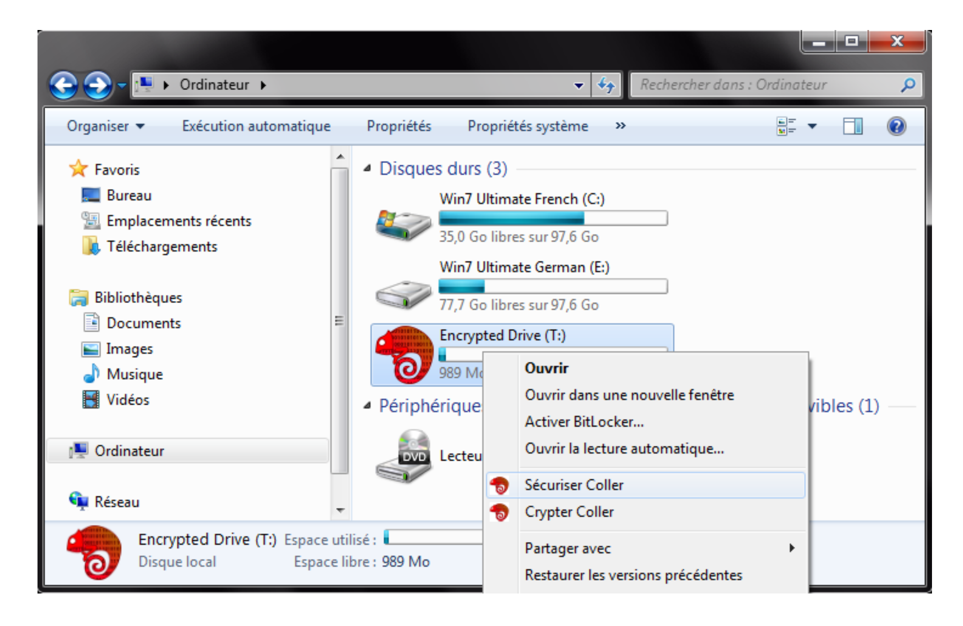


485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com



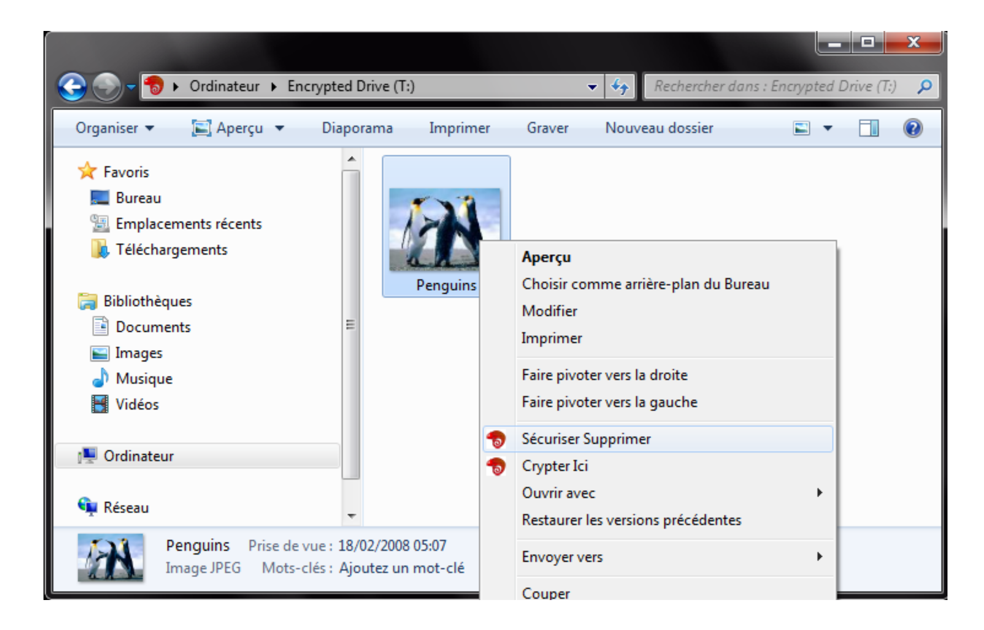

Vous pouvez également déplacer en sécurité un fichier vers le disque crypté en utilisant l’option « Sécuriser Coller ». Faites un clic droit sur le fichier ou dossier que vous souhaitez déplacer, puis sélectionner « Couper ». Ensuite, faites un clic droit sur un disque crypté ou sous-répertoire, puis sélectionnez « Sécuriser Coller ». Tout comme l’option Sécuriser Déplacer, la commande Sécuriser Coller élimine toute trace des fichiers non cryptés sur le disque dur.

Les commandes « Sécuriser » sont disponibles uniquement lorsque le dispositif Chameleon est connecté.




Le logiciel Chameleon fournit en plus une commande de suppression sécurisée. Faites un clic droit sur un fichier ou dossier puis sélectionnez « Sécuriser Supprimer ». L’utilisation de cette commande est plus sécurisée que la méthode consistant à supprimer le fichier une première fois

puis à le supprimer à nouveau dans la corbeille Windows. Puisque la commande « Sécuriser Supprimer » écrase le fichier dans sa totalité absolue à partir du disque dur, s'il s'agit d'une quantité de données importante, l'opération peut prendre un certain temps. Les commandes standards Couper, Coller et Supprimer de Windows restent disponibles.




Lors de sa suppression, un fichier enregistré sur un disque crypté sera déplacé vers la Corbeille Windows. Vous pouvez récupérer le fichier dans la corbeille tant que le dispositif Chameleon reste inséré. Les fichiers supprimés disparaissent de la corbeille lorsque le dispositif est retiré. Ils réapparaissent dans la corbeille lorsque le dispositif est réinséré. Il n'est pas nécessaire d'effectuer la commande « Sécuriser Supprimer » pour les fichiers se trouvant sur le disque crypté.

Tout fichier créé directement sur le disque crypté est automatiquement protégé. Certaines applications cependant, mettent des informations temporaires en mémoire dans votre disque non crypté. Il est possible de récupérer ces informations avec des outils spécialisés. Il est recommandé d'indiquer à vos applications de mettre leurs fichiers temporaires en mémoire dans le disque crypté. Ceci peut généralement se faire en installant vos applications directement sur le disque crypté.

Vous pouvez connecter ou déconnecter le dispositif Chameleon à n'importe quel moment. Votre ordinateur reste entièrement opérationnel même sans le dispositif Chameleon. Seul le disque crypté (ainsi que tous ses programmes et données) sera indisponible. Sachez que si vous débranchez le dispositif alors que les données sont en cours d'écriture au disque crypté, les données risquent d'être corrompues. Cette situation serait similaire à la déconnexion d'un disque dur externe alors qu'il serait en cours d'écriture. Afin d'être absolument certain qu'il n'y ait pas d'écriture en cours, utilisez la fonction « Retirer le périphérique en toute sécurité » de Windows avant de déconnecter le dispositif.




Si une application est ouverte avec un fichier crypté, cette application et ce fichier peuvent rester accessibles même après que vous ayez déconnecté le dispositif Chameleon. Prenons l’exemple d’un fichier Microsoft Word protégé sur lequel vous seriez en train de travailler. Si vous débranchez le dispositif, une copie de ce fichier reste ouverte dans Word. Vous ne pourrez pas enregistrer ce fichier sur le disque crypté jusqu’à ce que vous réinsériez le dispositif. Vous pouvez cependant visualiser et modifier les parties du fichier présentes en cache dans la mémoire de travail.

# 4 Gérer les Utilisateurs

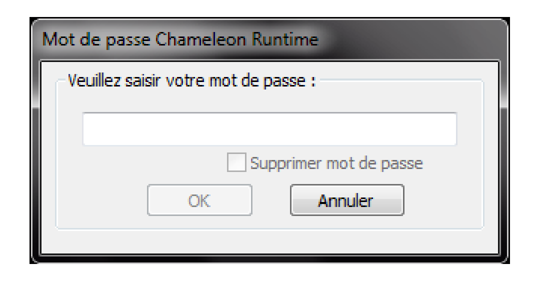
En plus des fonctions Chameleon principales, un Master peut créer des dispositifs Utilisateurs, y avoir accès, les dupliquer, paramétrer leurs termes et les verrouiller. Alors que les dispositifs Utilisateurs n’ont pas accès aux données protégées par d’autres dispositifs Utilisateurs, le Master, lui, peut accéder aux données protégées par n’importe quel Utilisateur (même lorsque les mots de passe ont été activés) auquel il est associé.

Un Master peut programmer uniquement des dispositifs Utilisateur entièrement nouveaux ou alors des utilisateurs qui à l’origine avaient été programmés par le même Master. Les Masters ne peuvent pas programmer un dispositif Utilisateur qui avait été programmé par un autre Master.

## *4.1 Créer des Dispositifs Utilisateurs*

1. **Connectez le dispositif Master**

2. **Saisissez votre mot de passe**




3. **Démarrez le Gestionnaire Chameleon**

Cliquez sur « Démarrer » de Windows >
Tous les programmes >
Chameleon >
Gestionnaire Chameleon





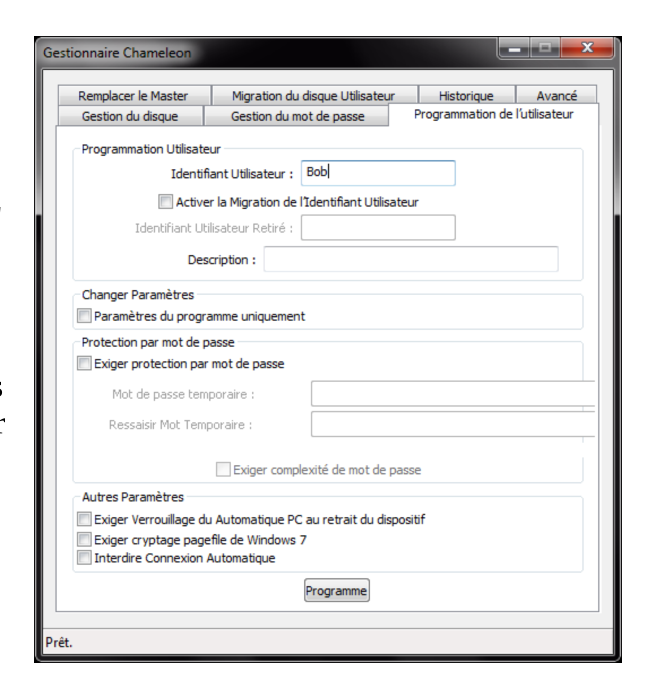


485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

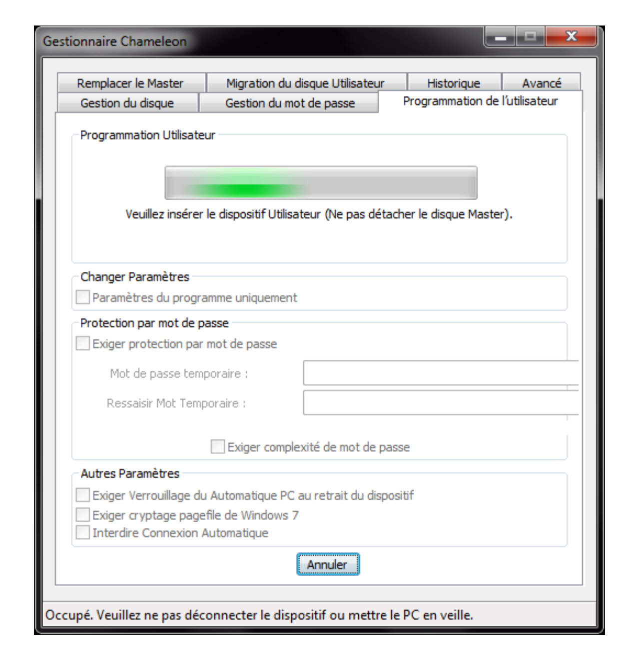
4. **Sélectionnez l'onglet « Programmation Utilisateur »**

   **Définissez l'identifiant Utilisateur** et les autres paramètres, puis **cliquez sur « Programme »**. Les sections suivantes décrivent les paramètres disponibles.

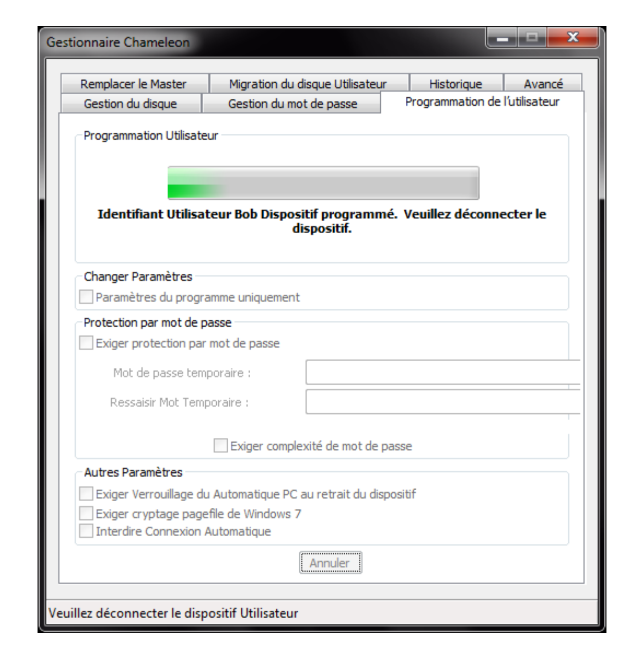
   Remarque : pour pouvoir changer les paramètres d'un dispositif Utilisateur sans changer l'identifiant Utilisateur et la description, sélectionnez la case à cocher **« Paramètres du programme seulement ».** Ne pas utiliser cette case à cocher sur un dispositif Utilisateur qui n'a pas été programmé auparavant.




5. **Connectez le dispositif Utilisateur** à programmer.



6. **Retirez le dispositif Utilisateur programmé** lorsque l'on vous le demande.




Les informations Utilisateur sont enregistrées sur le dispositif ainsi que sur un fichier texte non crypté dans le répertoire ChameleonDrives (par ex : C:\ChameleonDrives\UserLog.csv). Ces informations ne seront pas supprimées lorsque vous désinstallerez le logiciel Chameleon.

Vous pouvez reprogrammer un dispositif Utilisateur à n'importe quel moment. Les dispositifs Utilisateur peuvent être programmés uniquement pas le Master qui les avait programmés à l'origine ou alors par un double de ce Master.

### 4.1.1 Identifiant Utilisateur

Chaque dispositif Utilisateur est défini par un identifiant Utilisateur.  L'identifiant Utilisateur n'est pas secret et peut être composé de 31 chiffres et lettres maximum. Par exemple, l'identifiant Utilisateur peut être votre nom d'utilisateur, votre adresse e-mail ou votre numéro d'employé. Chaque identifiant Utilisateur est aussi lié à une description facultative. Cette description peut faire jusqu'à 255 caractères de long.

Les dispositifs Utilisateurs qui ont le même identifiant Utilisateur peuvent accéder aux mêmes données. Cela peut être utile pour faire des doubles ou alors pour donner accès à un groupe (plutôt qu'à une personne).

### 4.1.2 Mots de passe

Un mot de passe empêche les personnes non autorisées d'utiliser un dispositif Chameleon en particulier. Il ne sert pas à protéger les données. Lorsque la protection par mot de passe est activée, vous devez saisir un mot de passe à chaque fois que le dispositif est connecté ou que l'ordinateur redémarre ou sort du mode veille. Vous pouvez créer de multiples dispositifs Utilisateur, qui peuvent avoir chacun un mot de passe différent (ou pas de mot de passe), mais qui ont tous le même identifiant Utilisateur. Ces différents dispositifs Utilisateur peuvent accéder aux mêmes données.

Les Utilisateurs sont autorisés à changer leur mot de passe. Le Master peut exiger la complexité de mot de passe pour les mots de passe Utilisateur. Si la complexité de mot de passe est exigée, le mot de passe Utilisateur doit comporter un minimum de 6 caractères, y compris au moins un chiffre et une lettre.

Les mots de passe Utilisateur n'empêchent pas le Master d'avoir accès aux données cryptées par ses Utilisateurs.

### 4.1.3 Verrouillage PC (PC Lock)

En débranchant le dispositif Chameleon vos données confidentielles sont protégées, mais les documents ouverts, les connexions réseau et les e-mails peuvent rester vulnérables. Le PC Lock verrouille automatiquement la session Windows dès que le dispositif est retiré. L'utilisateur doit saisir un mot de passe Windows pour rouvrir la session Windows.

Un Master a la possibilité d'imposer à ses Utilisateurs l'utilisation de PC Lock.

### 4.1.4 Connexion Automatique (AutoLogin)

Le Chameleon Autologin est le contraire de PC Lock : une fois activé, vous pouvez ouvrir une session Windows tout simplement en branchant le dispositif Chameleon (voir « 11 Connexion Automatique (AutoLogin) » pour plus d'informations).

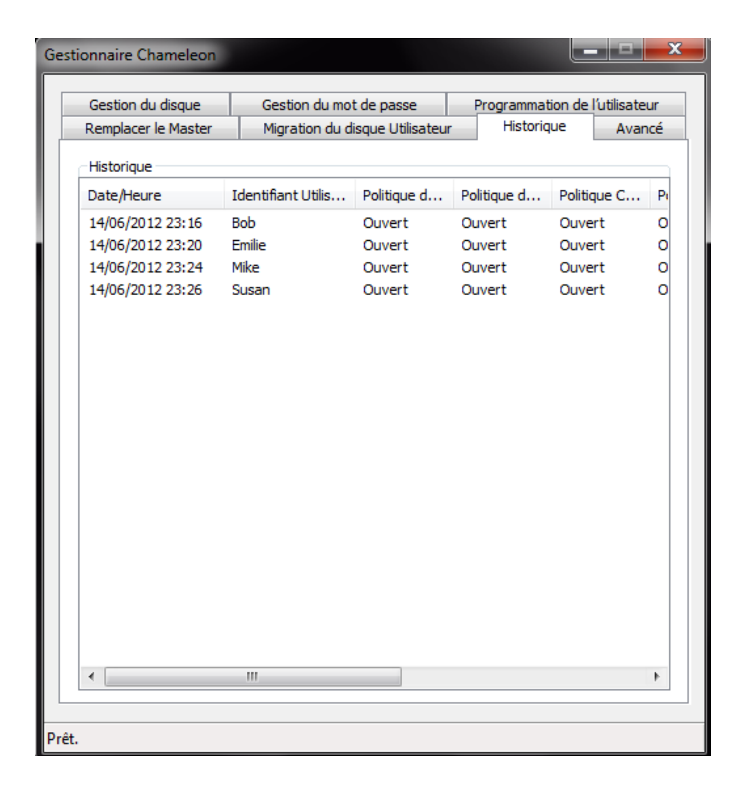
Un Master a la possibilité d'interdire à ses Utilisateurs d'utiliser AutoLogin.

### 4.1.5 Cryptage Pagefile

Windows peut sauvegarder des données temporaires dans son fichier de pagination (mémoire virtuelle). Ce fichier est généralement non crypté et apparaît sous la forme d'un amalgame de caractères qui est réactualisé continuellement. Activez le cryptage pagefile pour indiquer à Windows de crypter son fichier de pagination. Le cryptage du fichier de pagination élimine toute faille de sécurité potentielle, mais ralentit légèrement l'ordinateur. Seul Windows 7 permet le cryptage pagefile (ignoré pour les autres systèmes d'exploitation). Les Masters peuvent programmer les Utilisateurs afin que le cryptage pagefile soit obligatoire.

## *4.2 Journaux Utilisateurs*

L'onglet « Historique » montre la liste des dispositifs Utilisateur qui ont été créés. Cette information est enregistrée sur un fichier texte non crypté dans le répertoire ChameleonDrives (C:\ChameleonDrives\UserLog.csv). Il répertorie les dispositifs que le Master a créés, la date de leur création, l'identifiant Utilisateur, la description et les autres paramètres.

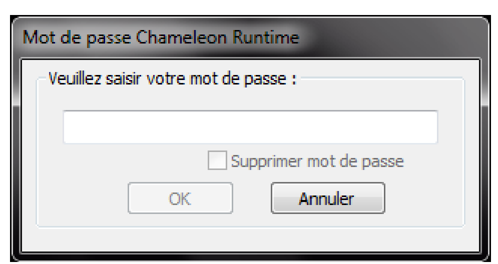



## 4.3 Utilisation du dispositif Chameleon sur plusieurs ordinateurs

Un dispositif Utilisateur peut être utilisé sur plusieurs ordinateurs. Si le logiciel Chameleon a déjà été installé sur le nouvel ordinateur, il n’est pas nécessaire de le réinstaller. Sinon insérez le CD d’installation Chameleon et exécutez le logiciel d’installation sur le nouvel ordinateur.

Le Master peut avoir accès aux disques de ses Utilisateurs :

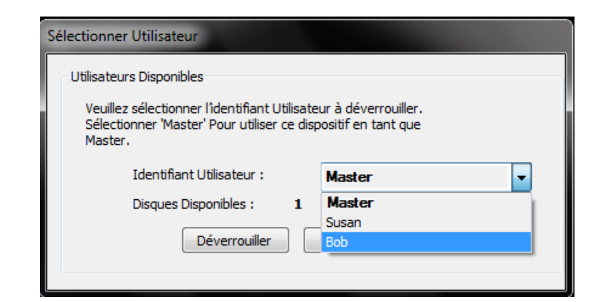
1. **Connectez le dispositif Master dans l’ordinateur qui contient le(s) disque(s) Utilisateur**
2. **Saisissez votre mot de passe**






485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

3. Dans la fenêtre « Sélectionner Utilisateur », **sélectionnez l'utilisateur** à qui appartiennent les disques auxquels vous voulez accéder. Puis, **cliquez sur « Déverrouiller ».**




Lorsqu'un Utilisateur associé est sélectionné, la fonctionnalité du Master est limitée à ce que l'Utilisateur peut faire.

Sélectionnez « Master » pour que le Master puisse utiliser la totalité de sa fonctionnalité Gérer les Utilisateurs.

## *4.4 Retirer définitivement des Utilisateurs*

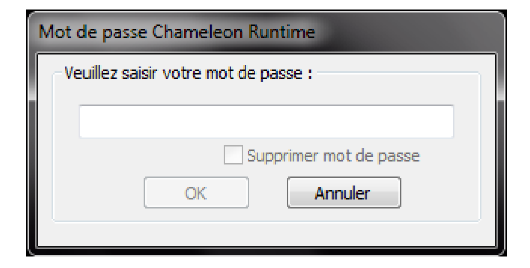
Lorsqu'un dispositif Utilisateur est perdu, ou lorsqu'un employé possédant un dispositif Utilisateur quitte l'entreprise, il s'avère nécessaire de retirer définitivement l'Utilisateur et son dispositif. Ceci peut s'effectuer de différentes façons :

- Si les données appartenant à l'Utilisateur ne sont plus nécessaires, alors les disques appartenant à l'Utilisateur peuvent être supprimés et le dispositif Utilisateur peut être programmé avec un nouvel identifiant Utilisateur. Voir « `4.4.1 Supprimer des disques Utilisateur` ».
- Si vous souhaitez faire migrer les disques de l'Utilisateur retiré vers un autre identifiant Utilisateur, vous pouvez :
    - Utiliser le Master (Voir « `4.4.2Changer d'utilisateur avec un Master` »)
    - Créer un dispositif Utilisateur pour lequel les migrations sont activées (Voir « `4.4.3 Changer d'utilisateur avec un dispositif Utilisateur Migration`
    - ).

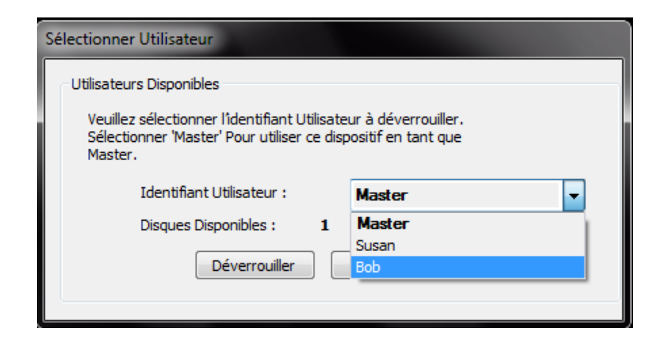
### 4.4.1 Supprimer des disques Utilisateur

1. **Connectez le dispositif Master dans l'ordinateur contenant le(s) disque(s) Utilisateur.**

2. **Saisissez votre mot de passe**



3. Dans la fenêtre « Sélectionner Utilisateur », **sélectionnez l'utilisateur** à qui appartiennent les disques que vous souhaitez supprimer. Puis **cliquez sur « Déverrouiller ».**



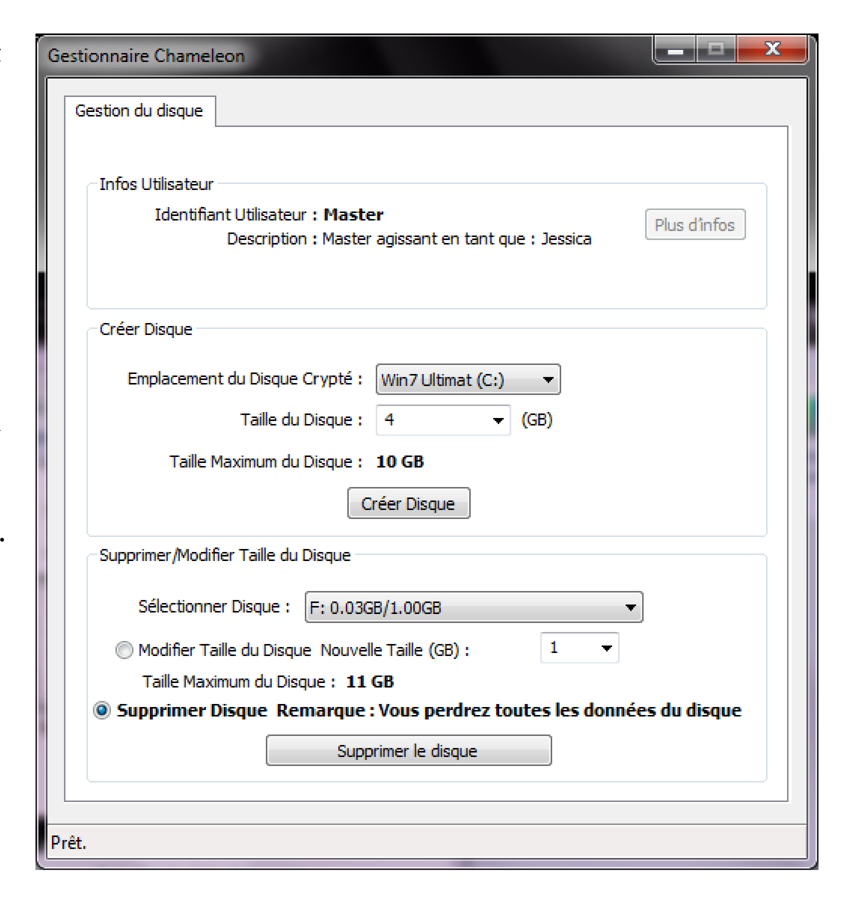

4. **Démarrer le Gestionnaire Chameleon**

Cliquez sur « Démarrer » de Windows >
Tous les programmes >
Chameleon >
Gestionnaire Chameleon

5. **Sélectionnez l'onglet « Gérer Disque »**.

6. Dans la section du disque « Supprimer /Redimensionner », **sélectionnez « Supprimer le disque »**.

7. **Cliquez** sur le bouton **« Supprimer le disque »** pour chaque disque de l'utilisateur.



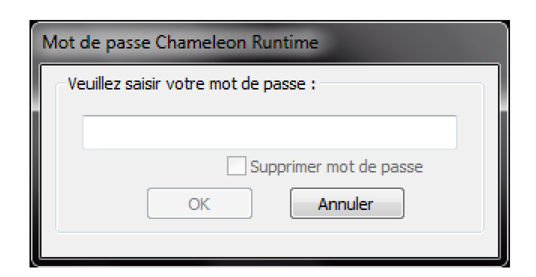

## 4.4.2 Changer d'utilisateur avec un Master



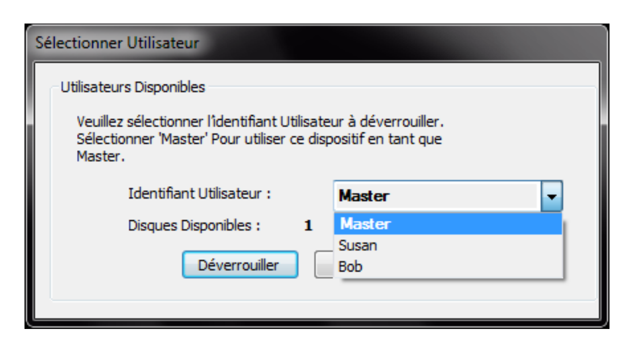

485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

1. **Connectez le Master dans l'ordinateur contenant le(s) disque(s) crypté(s) de l'Utilisateur.**

2. **Saisissez votre mot de passe**




3. Dans la fenêtre « Sélectionner Utilisateur », **sélectionnez « Master »** et **cliquez sur « Déverrouiller »**



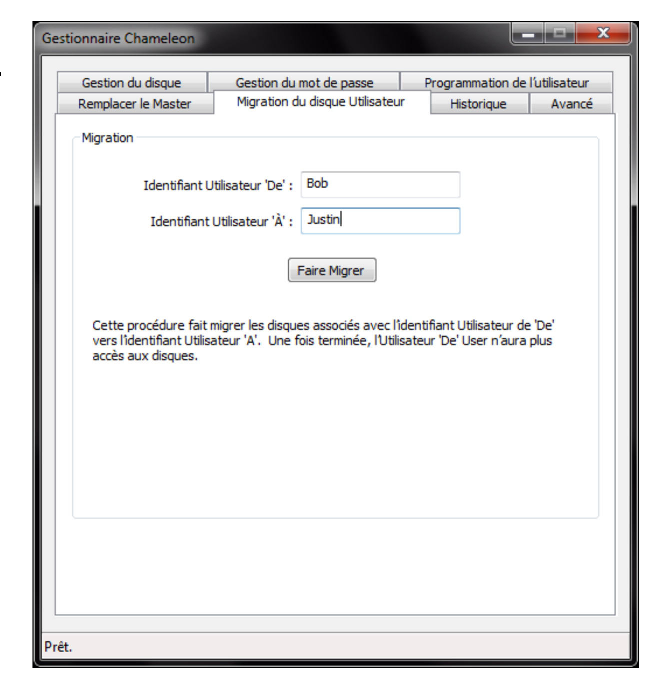

4. **Démarrez le Gestionnaire Chameleon**

Cliquez sur « Démarrer » de Windows >
Tous les programmes >
Chameleon >
Gestionnaire Chameleon

5. **Sélectionnez l'onglet « Migration Disque Utilisateur »**.

6. Saisissez l’identifiant Utilisateur existant dans « Identifiant Utilisateur ’De’ » et le nouvel Identifiant Utilisateur dans « Identifiant Utilisateur ’À’ ».

   Pour verrouiller tous les Utilisateurs existants, saisissez « Inutilisé » pour l’Identifiant Utilisateur « De ».




7. **Cliquez sur le bouton « Migrer »**.

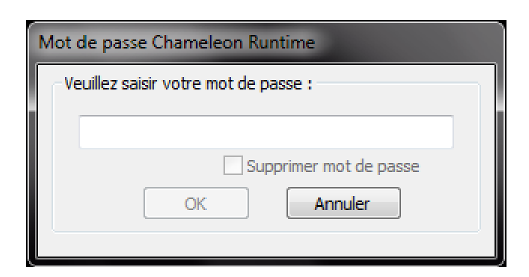
Votre disque dur (C:\) doit avoir assez d’espace libre pour pouvoir contenir tous les fichiers des disques cryptés. Selon le volume des données cryptées, il se peut que ce processus prenne un certain temps.

Tous les disques cryptés non connectés (ainsi que les copies de sauvegarde) resteront accessibles par l’Utilisateur d’origine. Vous pouvez répéter ce processus lorsque ces disques seront connectés. Ce processus n’entraîne pas la migration et ne verrouille pas l’accès aux fichiers cryptés individuellement. (Voir `7.3 Faire migrer des fichiers cryptés`).

### 4.4.3 Changer d’utilisateur avec un dispositif Utilisateur Migration

1. **Connectez le Master**

2. **Saisissez votre mot de passe**




3. **Démarrer le Gestionnaire Chameleon**

   Cliquez sur « Démarrer » de Windows > Tous les programmes >







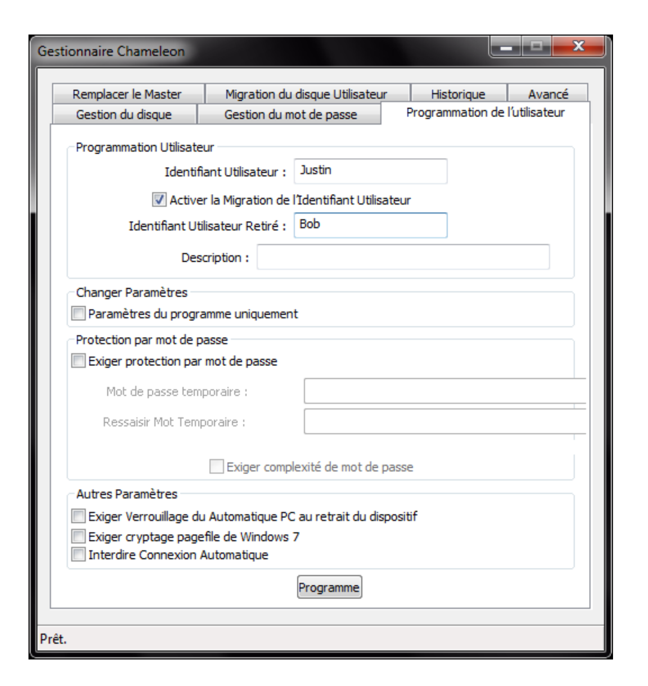
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

Chameleon >
Gestionnaire Chameleon

4. **Sélectionner l'onglet « Programmation Utilisateur ».**

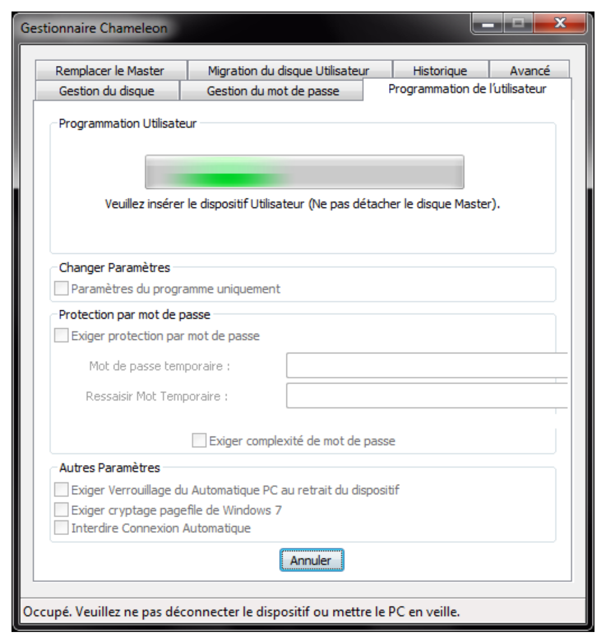
   **Sélectionnez la case à cocher « Activer migration d'Identifiant Utilisateur ».**

   Saisissez le nouvel identifiant Utilisateur, l'identifiant Utilisateur retiré et les autres paramètres Utilisateur. Tout ce que appartenait à l'identifiant Utilisateur retiré sera transféré vers le nouvel identifiant Utilisateur.




5. **Cliquez sur le bouton « Programmer ».**

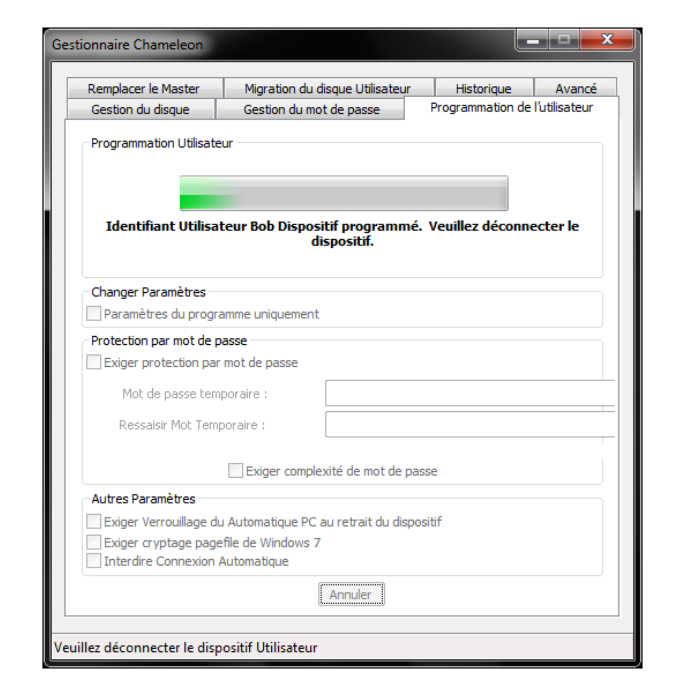
6. **Connectez le dispositif Utilisateur** à programmer.






485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

7. **Retirez le dispositif Utilisateur programmé** lorsque l’on vous le demande.




Lorsque l’utilisateur insère dans son PC ce dispositif Utilisateur pour lequel la migration est activée, on lui demandera d’exécuter le Gestionnaire Chameleon. Le Gestionnaire Chameleon entraîne automatiquement la migration des disques cryptés de l’utilisateur retiré vers le nouvel identifiant Utilisateur. Le disque dur contenant le dossier Windows temporaire (généralement C:\) doit avoir assez d’espace libre pour pouvoir contenir tous les fichiers des disques cryptés. Selon le volume des données cryptées, il se peut que ce processus prenne un certain temps.

Une fois la migration terminée, le dispositif Utilisateur pour lequel la migration est activée fonctionne comme un dispositif Utilisateur standard.

Tous les disques cryptés non connectés (ainsi que les copies de sauvegarde) resteront accessibles par l’identifiant Utilisateur retiré. On demandera à l’utilisateur de les faire migrer lorsqu’ils seront connectés ultérieurement. Les disques cryptés n’ayant pas migré ne sont pas automatiquement chargés avec le dispositif Utilisateur pour lequel la migration est activée. Ils devront migrer vers le nouvel identifiant Utilisateur.

Ce processus n’entraîne pas la migration et ne verrouille pas l’accès aux fichiers cryptés individuellement (voir « 7.3 Faire migrer des fichiers cryptés »).

# 5 Dupliquer un dispositif Master

Si vous perdez ou cassez votre dispositif Master, les données du disque crypté peuvent être récupérées en utilisant un nouveau dispositif Master et la phrase de passe de récupération que vous aviez indiquée pendant l’installation. Ce processus peut également être utilisé pour créer des doubles du dispositif Master. Les Masters sans phrase de passe de récupération ne peuvent pas être dupliqués.



485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

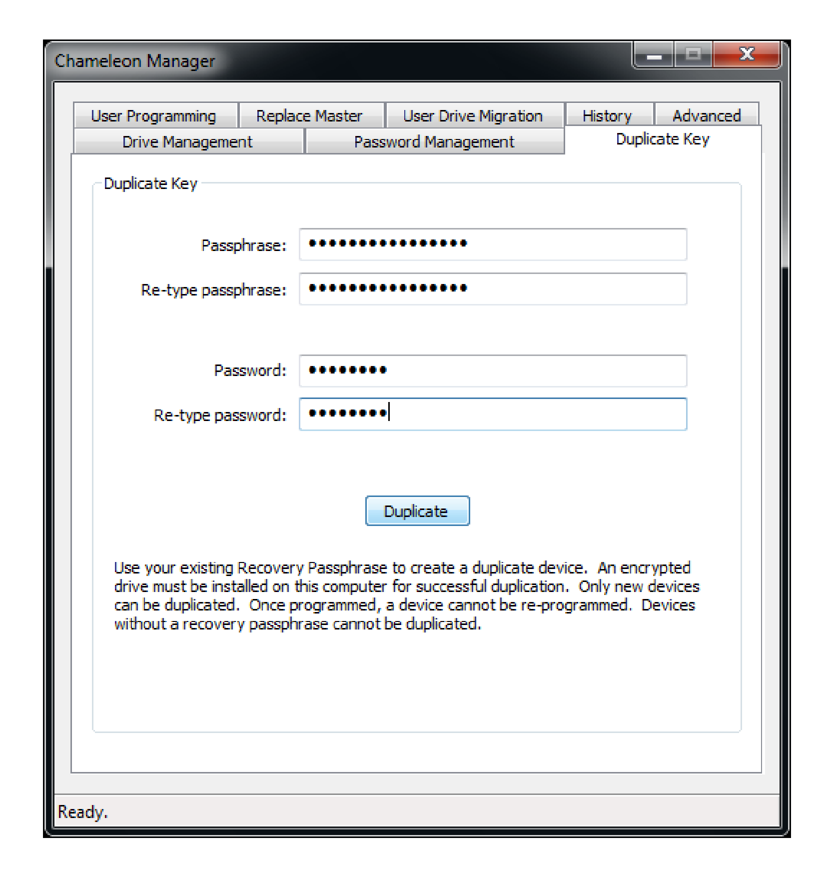
1. **Connectez un nouveau dispositif Master** dans un PC contenant un disque crypté associé au Master à dupliquer.

2. **Démarrez le Gestionnaire Chameleon**

   Cliquez sur « Démarrer » de Windows >
   Tous les programmes >
   Chameleon >
   Gestionnaire Chameleon

3. **Dans l’onglet « Dupliquer Clé », saisissez votre phrase de passe de récupération d’origine,** ainsi qu’un **mot de passe de votre choix.**

4. **Cliquez sur le bouton « Dupliquer »**.




Vous n’avez pas besoin du Master d’origine pour créer un double. Mais par précaution, un disque crypté associé au Master à dupliquer doit être présent afin d’assurer la réussite de la duplication. Le Gestionnaire Chameleon vérifiera que la phrase de passe saisie corresponde bien au disque crypté Master existant avant d’autoriser la phrase de passe à assigner au dispositif.

# 6 Remplacer un Master

Dans le cas où un dispositif Master serait perdu, volé, ou compromis, il peut s’avérer nécessaire de remplacer le Master et de recrypter toutes les données associées. Ce processus inclus :

- la réactualisation de la clé de cryptage du dispositif Master
- la migration des disques cryptés Master associés vers la nouvelle clé de cryptage
- la réactualisation de tous les dispositifs Utilisateur afin qu’ils correspondent à la nouvelle clé de cryptage Master

- la migration de tous les disques Utilisateur cryptés[3]
- la migration des fichiers .cge Master et Utilisateur vers les clés réactualisées (Voir `7.3 Faire migrer des fichiers cryptés` pour plus d'informations)

Chaque dispositif Master ne peut être réactualisé qu'une seule fois après avoir été programmé. Vous aurez besoin d'un nouveau Dispositif Master pour répéter cette procédure.

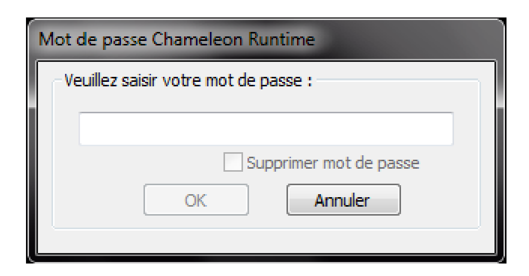
Avant de remplacer le Master:

- Créez une copie de sauvegarde d'un disque crypté appartenant au Master (Voir « 12.4 `Créer des copies de sauvegarde des données` ») : ceci autorisera à l'avenir la création de doubles du Master d'origine. Le disque peut être de la taille minimum.
- Créez des doubles du dispositif Master actuel (Voir « 5 `Dupliquer un dispositif Master` »).
    - Tous les doubles créés après que le dispositif Master ait été remplacé ne contiennent pas la clé d'origine. Par conséquent, ils ne pourront pas accéder aux disques associés avec l'original et ne pourront pas non plus programmer les dispositifs Utilisateur avec leurs clés d'origine correspondantes.
- Effectuez la procédure de remplacement ci-dessous sur le dispositif Master (ainsi que tous ses doubles)

Pour remplacer le dispositif Master :

1. **Connectez le dispositif Master** à remplacer.

2. **Saisissez votre mot de passe**




3. **Démarrez le Gestionnaire Chameleon**

Cliquez sur « Démarrer » de Windows >
Tous les programmes >
Chameleon >
Gestionnaire Chameleon

[3] Y compris les copies de sauvegarde

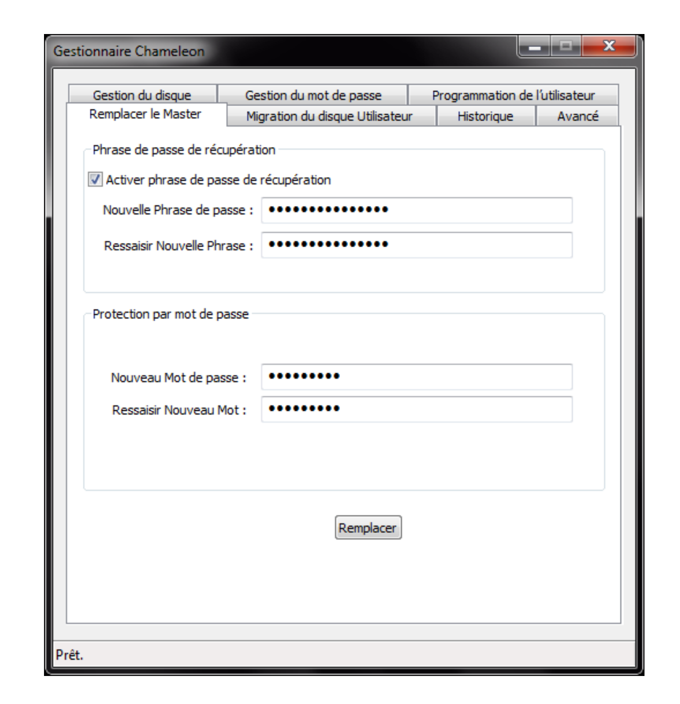



4. **Sélectionnez l'onglet « Remplacer le Master »**.

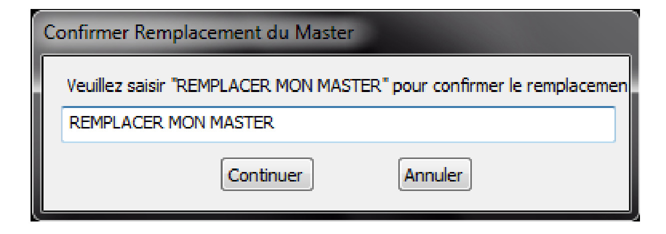
5. **Saisissez la nouvelle phrase de passe de récupération**. (Reportez-vous à la rubrique 2 concernant le choix d'une phrase de passe de récupération).

6. **Saisissez un mot de passe**.

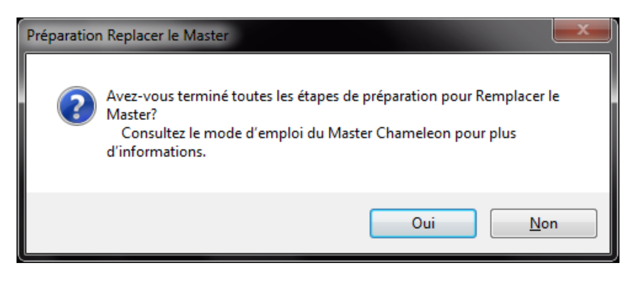
7. **Cliquez sur « Remplacer »**.



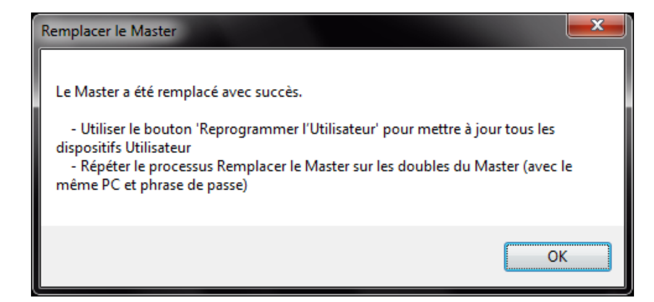

8. **Saisissez la phrase de confirmation**.




9. **Confirmez la préparation**.




10. Lorsque les disques du Master auront migré vers la nouvelle clé, le gestionnaire affichera le rappel suivant.



Par précaution, un disque Master crypté doit être associé à la phrase de passe actuelle (ancienne) ou à la phrase de passe saisie récemment afin d'assurer la réussite du remplacement.

Cette procédure de remplacement fait également migrer tous les disques Master cryptés qui sont connectés (disques cryptés qui sont accessibles uniquement par le Master) vers la nouvelle clé de cryptage du Master. Le disque dur contenant le dossier temporaire Windows (généralement C:\) doit avoir assez d'espace libre pour pouvoir contenir tous les fichiers des disques cryptés. Selon le volume des données cryptées, il se peut que ce processus prenne un certain temps.

Après avoir remplacé le premier dispositif Master:

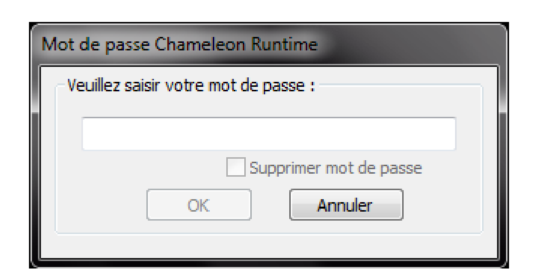
- **Répétez le processus de remplacement du Master sur les doubles du dispositif Master qui sont sur le même PC et qui ont la même phrase de passe.** Ceci garantira la transition de tous les doubles vers la même phrase de passe.
- **Réactualisez tous les dispositifs Utilisateur associés**. Voir la section suivante.
- **Faites migrer tous les disques Master sur les autres PC.** Connectez simplement le Master réactualisé et ouvrez le Gestionnaire Chameleon.
- **Faites migrer tous les disques Master cryptés qui se trouvent sur des disques externes**. On vous demandera de les faire migrer lorsqu'ils seront connectés ultérieurement.
- Après la migration de disques cryptés, **créez leurs nouvelles copies de sauvegarde** afin de remplacer les anciennes copies de sauvegarde.
- **Faites migrer les fichiers cryptés individuellement associés au Master** (Voir « 7.3 Faire migrer des fichiers cryptés »).

## *6.1 Réactualisation des dispositifs Utilisateur*

Utilisez le dispositif Master réactualisé pour reprogrammer tous les dispositifs Utilisateur.

1. **Connectez le Master**.

2. **Saisissez votre mot de passe**

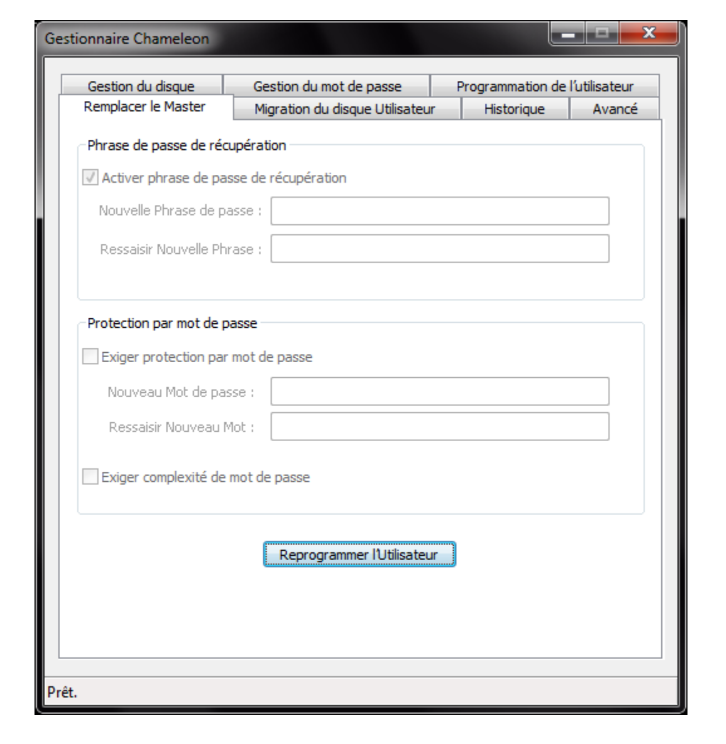



3. **Démarrez le Gestionnaire Chameleon**

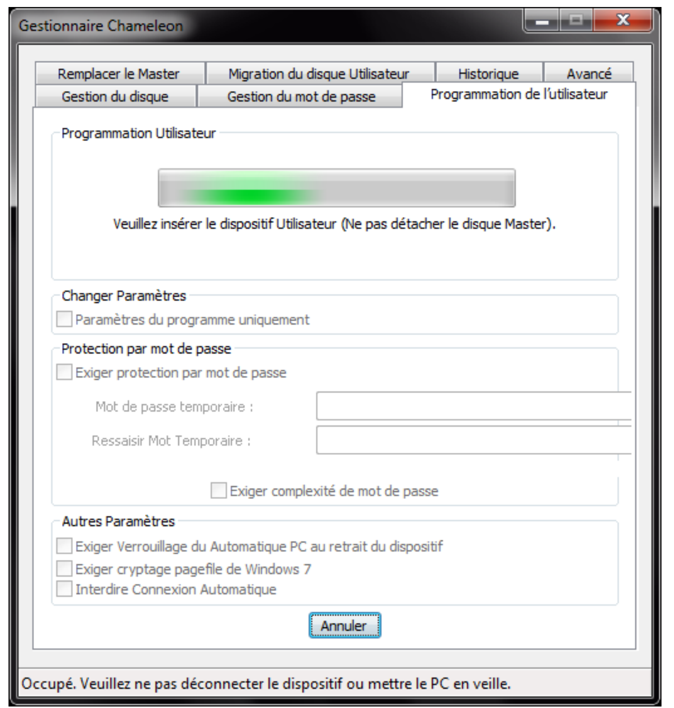
Cliquez sur « Démarrer » de Windows >
Tous les programmes >
Chameleon >
Gestionnaire Chameleon

4. **Sélectionnez l'onglet « Remplacer le Master »**.

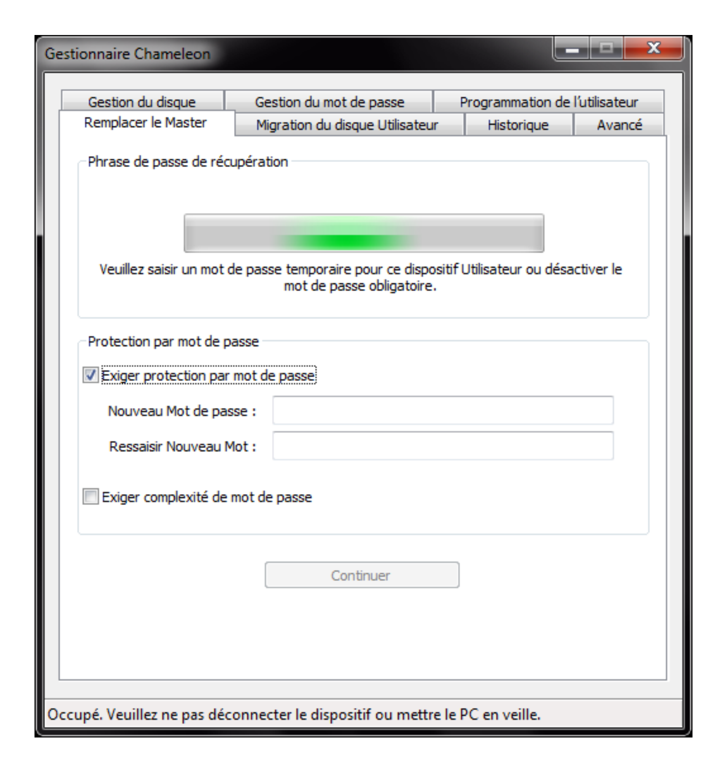
5. **Cliquez sur « Reprogrammer Utilisateur »**.



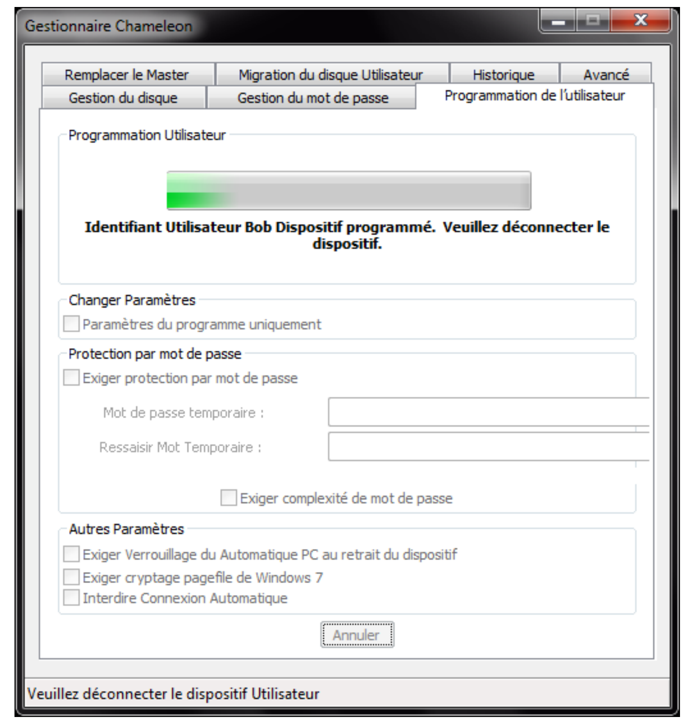

6. **Connectez le dispositif Utilisateur** à reprogrammer.



7. Si un mot de passe était exigé auparavant sur le dispositif Utilisateur, **saisissez un nouveau mot de passe temporaire** ou désactivez le mot de passe obligatoire.




8. **Retirez le dispositif Utilisateur programmé** lorsque l'on vous le demande.




Lorsque l'utilisateur insère dans son PC le dispositif Utilisateur réactualisé, on lui demandera d'exécuter le Gestionnaire Chameleon. Le Gestionnaire Chameleon entraîne automatiquement la migration des disques cryptés associés afin de correspondre au Master réactualisé. Le disque dur contenant le dossier Windows temporaire (généralement C:\) doit avoir assez d'espace libre pour

pouvoir contenir tous les fichiers des disques cryptés. Selon le volume des données cryptées, il se peut que ce processus prenne un certain temps.
Ce processus ne fait pas migrer et ne verrouille pas l'accès aux fichiers cryptés individuellement (voir 7.3 `Faire migrer des fichiers cryptés`).

Tous les disques cryptés non connectés (ainsi que les copies de sauvegarde) resteront accessibles par le dispositif Utilisateur d'origine. On demandera à l'utilisateur de les faire migrer lorsqu'ils seront connectés ultérieurement. Les disques cryptés n'ayant pas migré ne seront pas accessibles jusqu'à ce que le dispositif Utilisateur réactualisé les ait fait migré.

# 7 Crypter des fichiers et dossiers individuels

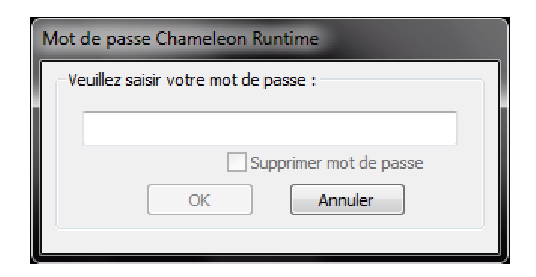
Le dispositif Chameleon crypte automatiquement toutes les données placées dans le disque crypté et décrypte automatiquement toutes les données enlevées du disque crypté. Bien que pratique et sécurisé, ceci ne protège pas les informations envoyées par e-mail ou mises en mémoire sur Internet. Dans de telles situations, le dispositif Chameleon peut crypter et décrypter des fichiers et dossiers individuels.

## *7.1 Crypter des fichiers*

Vous pouvez crypter un fichier seul, un groupe de fichiers ou des répertoires entiers (mais pas les raccourcis ou icônes spéciaux comme la corbeille Windows). Les fichiers cryptés par un dispositif Chameleon ne peuvent être décryptés qu'en utilisant le même dispositif (ou par son Master).

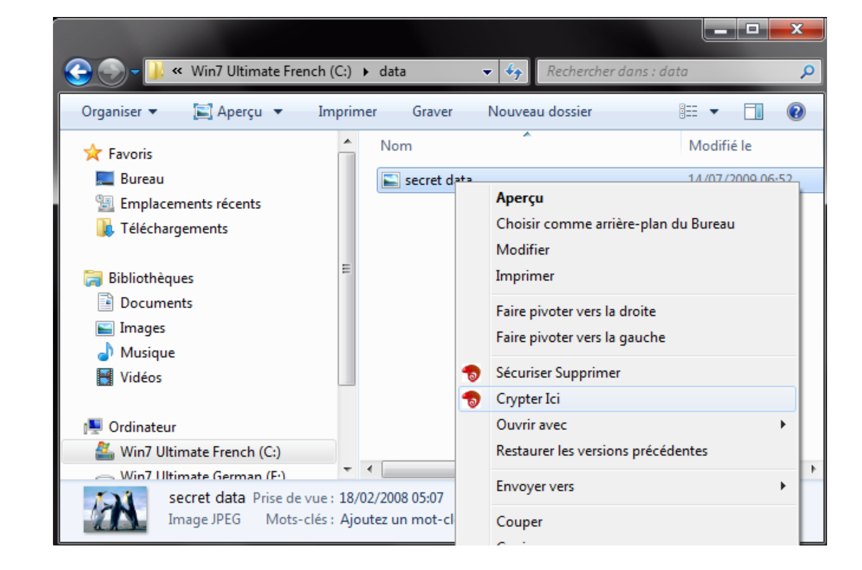
1. **Connectez le dispositif Master**

2. **Saisissez votre mot de passe**



3. **Faites un clic droit sur le fichier** ou dossier que vous souhaitez protéger.

4. **Sélectionnez « Crypter ici »** pour créer une version cryptée du fichier sélectionné

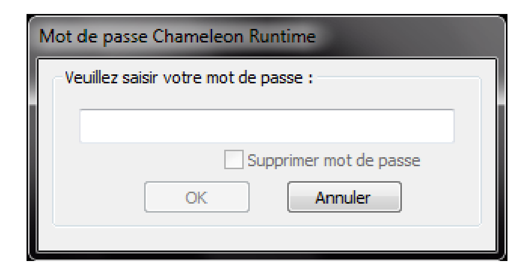



Le fichier crypté apparaîtra comme fichier du même dossier avec le même nom de fichier, mais avec l'extension « .cge ». Si vous le souhaitez, vous pouvez changer le nom du fichier, mais pas l'extension. Ce fichier est crypté grâce au hardware AES-256 du dispositif. Contrairement au disque crypté, le fichier crypté reste visible quand le dispositif est retiré. Il peut être joint à un e-mail, copié vers un disque USB, mis en mémoire dans le réseau ou alors synchronisé à un service Cloud.

Vous pouvez également crypter des fichiers et dossiers individuels en utilisant un « glisser-déposer » effectué avec un clic droit.

1. **Connectez le dispositif Master**

2. **Saisissez votre mot de passe.**

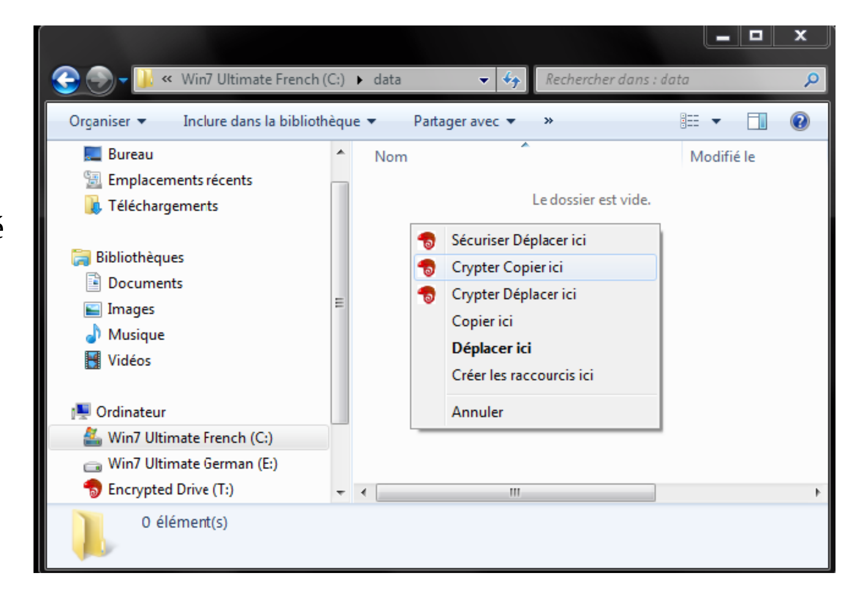



3. **Cliquez et maintenez appuyé le bouton droit de la souris sur le fichier ou dossier que vous souhaitez protéger.**



485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

4. **Faites glisser le pointeur de la souris vers le dossier cible et relâchez le bouton droit de la souris.** Le fichier crypté sera créé dans ce dossier.



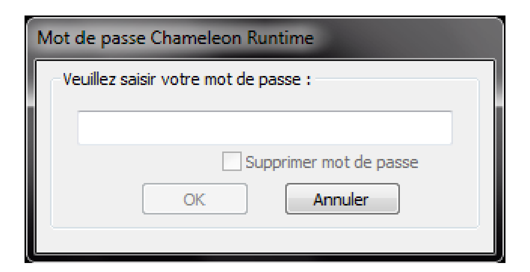

5. **Sélectionnez « Crypter Déplacer ici» ou « Crypter Copier ici»**.
« Crypter Déplacer ici» place le fichier crypté dans l'emplacement choisi tout en supprimant le fichier source en sécurité.

   « Crypter Copier ici » fait la même chose, mais sans supprimer le fichier source.

Vous pouvez également crypter un fichier ou dossier en utilisant l'option du Coller crypté :

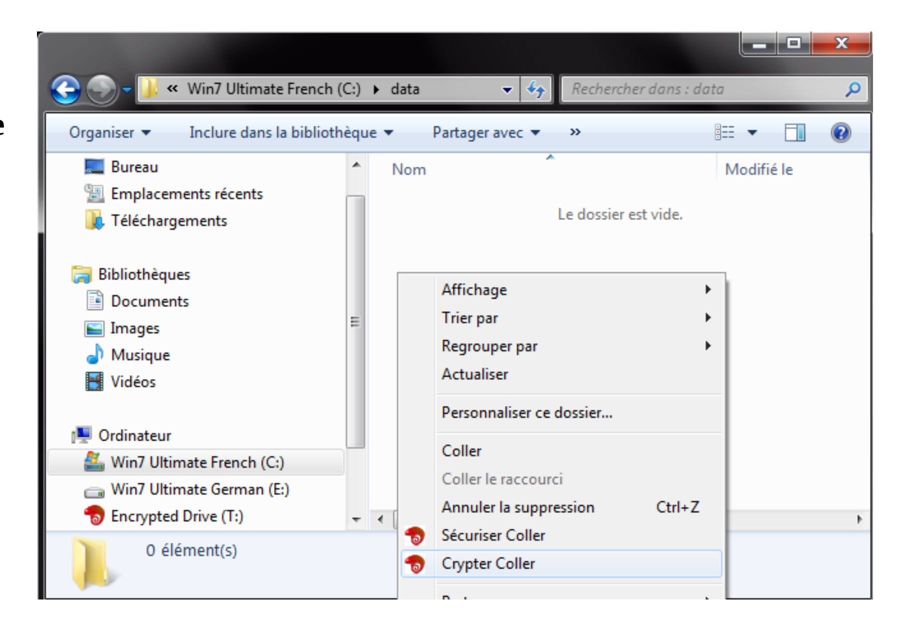
1. **Connectez le dispositif Master**

2. **Saisissez votre mot de passe**




3. **Faites un clic droit sur le fichier ou dossier** que vous souhaitez crypter, puis **sélectionnez « Couper » ou « Copier »**. Vous pouvez également utiliser les raccourcis du clavier Couper (CTRL+x) ou Copier (CTRL+c).

4. **Faites un clic droit le disque ou répertoire de destination.**




5. **Sélectionnez « Crypter Coller »**

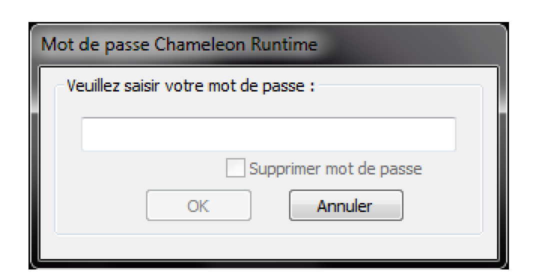
Ceci déplace le fichier crypté vers la destination. Si vous aviez sélectionné « Couper », le fichier source sera supprimé en sécurité une fois le cryptage terminé.

## *7.2 Décrypter des dossiers*

Pour décrypter un fichier .cge :

1. **Connectez le dispositif Master**

2. **Saisissez votre mot de passe (si activé)**



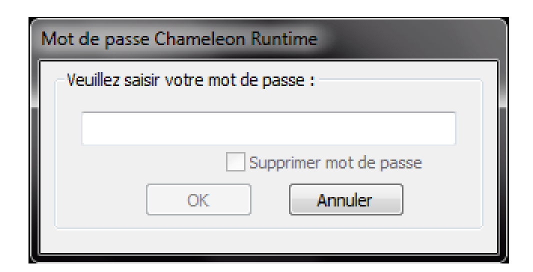

3. **Double cliquez sur le fichier .cge**.
   Le processus de décryptage commencera immédiatement.

Remarque : si vous ouvrez le fichier .cge à partir d'une application (telle qu'un navigateur Internet) en utilisant (par exemple) « Ouvrir avec », alors le fichier sera téléchargé et décrypté dans un dossier temporaire choisi par l'application. Ceci déplacera le contenu décrypté du fichier .cge dans un dossier imprévu. Au lieu d'ouvrir le fichier .cge directement à partir de l'application, enregistrez-le dans un dossier de votre choix (en utilisant « Enregistrer sous ») et décryptez-le ensuite.

Les autres méthodes de décryptage de fichiers .cge sont approximativement les mêmes que les méthodes de cryptage :

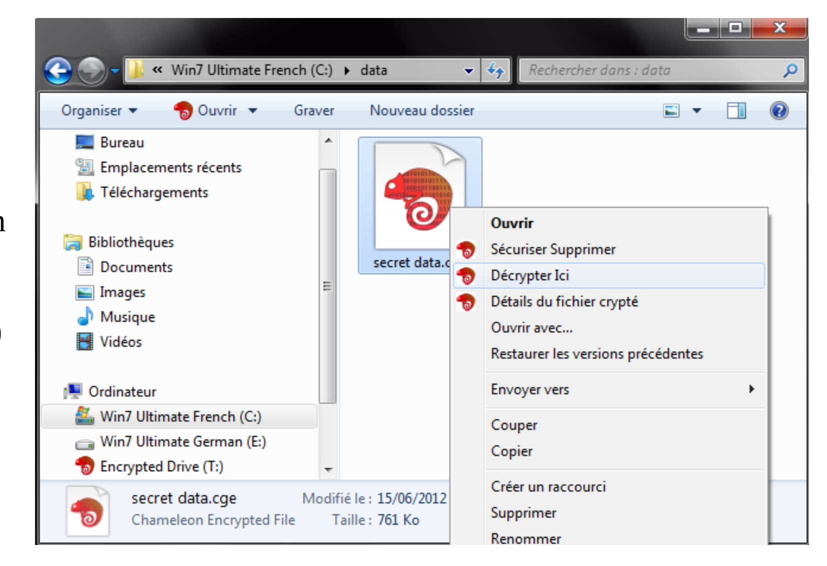
1. **Connectez le dispositif Master**

2. **Saisissez votre mot de passe**




3. **Faites un clic droit sur fichier .cge** à décrypter.

4. **Sélectionnez « Décrypter ici »** afin de créer une copie du(des) fichier(s) ou dossier(s) décryptés(s) contenus dans le fichier .cge.



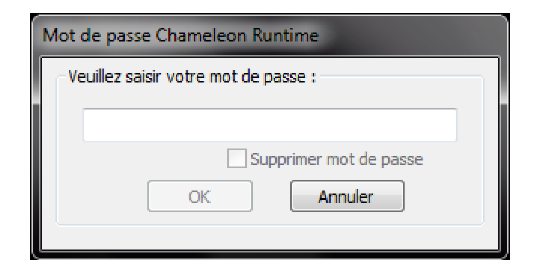




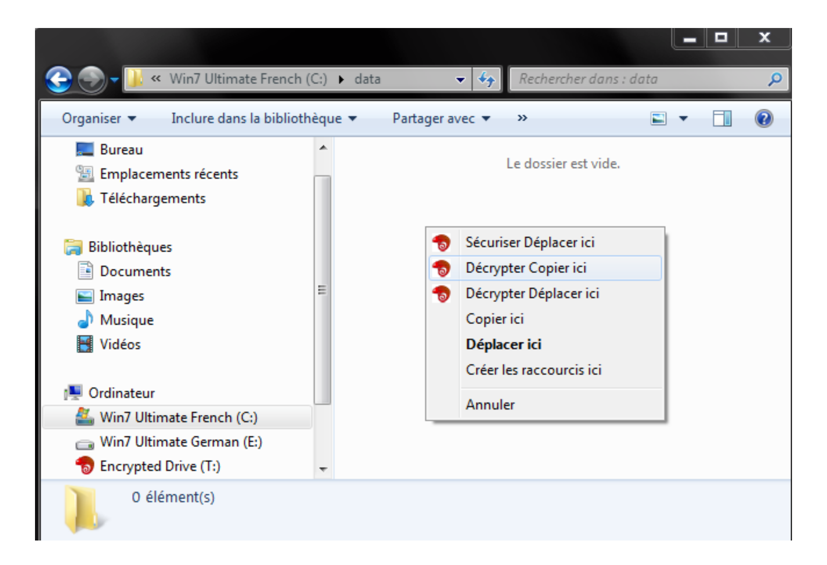
485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

De la même manière, vous pouvez décrypter des fichiers .cge en utilisant la méthode « glisser-déposer » avec un clic droit. Utilisez cette méthode lorsque le fichier .cge se trouve dans une mémoire non sécurisée. Cette méthode est plus fiable car elle permet d'éviter que vos données non cryptées résident (temporairement) dans la mémoire non sécurisée. Prenons l'exemple d'un fichier .cge enregistré sur une unité de réseau. Au lieu de double cliquer sur le fichier afin de le décrypter sur le dossier réseau, vous pouvez utiliser la méthode suivante pour décrypter le fichier sur votre disque dur local.

1. **Connectez le dispositif Master**
2. **Saisissez votre mot de passe**




3. **Cliquez et maintenez appuyé le bouton droit de la souris sur le fichier .cge**
4. **Faites glisser le pointeur de la souris** vers le dossier cible et et relâchez le bouton droit de la souris. Le contenu décrypté sera créé dans ce dossier.




5. **Sélectionnez « Décrypter Déplacer ici» ou « Décrypter Copier ici ».**
   « Décrypter Déplacer ici» déplace le contenu décrypté vers la destination tout en supprimant le fichier .cge en sécurité. Il est conseillé d'utiliser cette méthode afin d'éviter que vos données non cryptées résident (temporairement) dans une mémoire non sécurisée ou distante.

   « Décrypter Copier ici » fait la même chose, mais sans supprimer le fichier source.

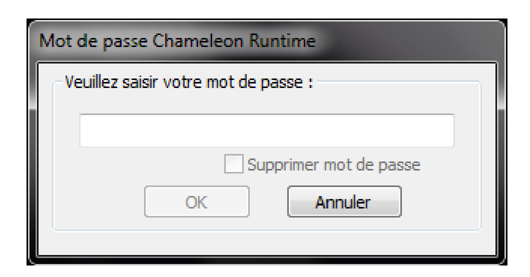
L'option Décrypter Coller est également disponible :




485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

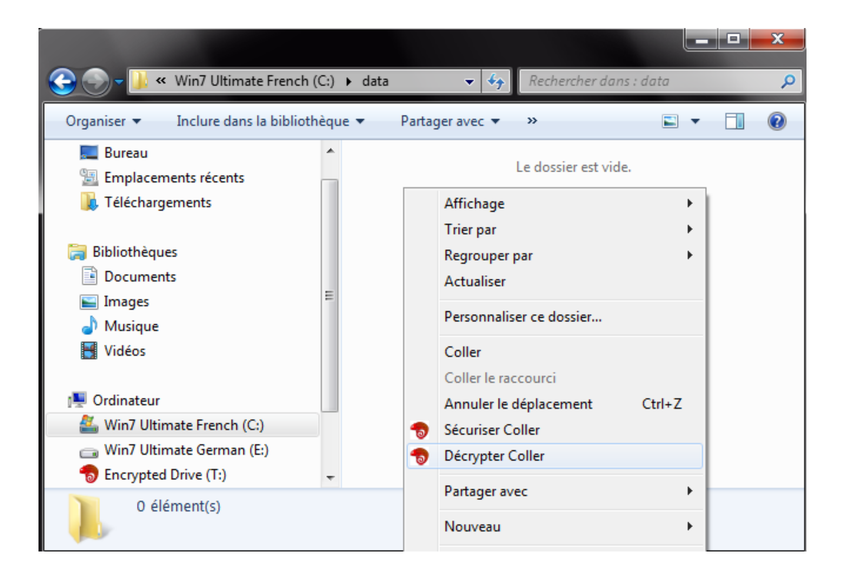
1. **Connectez le dispositif Master**

2. **Saisissez votre mot de passe**




3. **Faites un clic droit sur fichier .cge file** à décrypter, puis **sélectionnez « Couper » ou « Copier »**. Vous pouvez également utiliser les raccourcis Couper (CTRL+x) ou Copier (CTRL+c) du clavier.

4. **Faites un clic droit sur le disque ou répertoire de destination.**




5. **Sélectionnez « Décrypter Coller »**

Ceci déplace le contenu décrypté vers la destination. Si « Couper » avait été sélectionné, le fichier source sera supprimé en sécurité une fois le décryptage terminé.

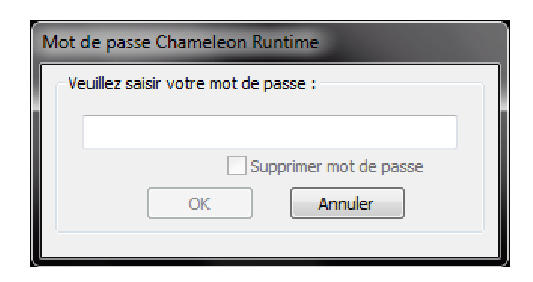
## *7.3 Faire migrer des fichiers cryptés*

Il existe plusieurs cas de figure dans lesquels il est nécessaire de faire migrer des fichiers .cge :

- Le dispositif Master a été remplacé : dans ce cas, le Master ou l'Utilisateur associé devra faire migrer les fichiers .cge cryptés avec la clé d'origine (Voir « 6 Remplacer un Master »)
- Le Master a besoin d'accéder aux fichiers d'un Utilisateur associé
- Un Utilisateur est retiré définitivement : un dispositif Utilisateur pour lequel la migration a été activée peut transférer la possession d'un fichier .cge de l'utilisateur retiré au nouvel Utilisateur (Voir « 4.4.3 Changer d'utilisateur avec un dispositif Utilisateur Migration »).

1. **Connectez le dispositif**
   (Cela peut être un Master réactualisé, un Utilisateur réactualisé, ou un Utilisateur pour lequel la migration a été activée)

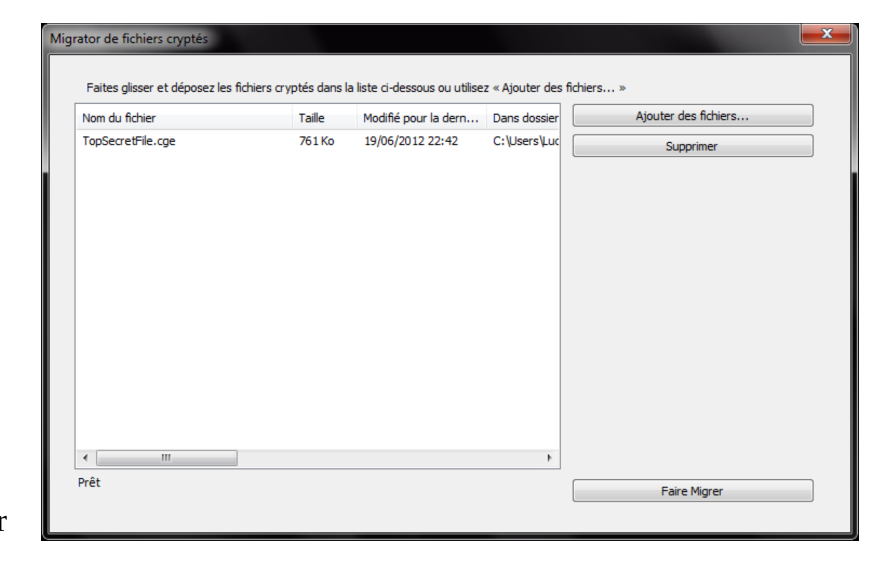
2. **Saisissez votre mot de passe** (si activé)




3. **Démarrer le « Migrator de fichiers cryptés »**

   Cliquez sur « Démarrer » de Windows >
   Tous les programmes >
   Chameleon >
   Migrator de Fichiers Cryptés

4. **Sélectionnez les fichiers .cge à faire migrer.**




   Faites-les glisser directement vers la liste des fichiers du Migrator Chameleon

   ou alors

   Cliquez sur « Ajouter des fichiers », naviguez et sélectionnez les fichiers.

5. **Fermez tous les fichiers ouverts qui résident dans les disques cryptés.**

   Avant que le processus de migration ne commence, les disques cryptés seront détachés. Si un fichier est ouvert le Migrator demandera à l'utilisateur de le fermer.

6. **Cliquez sur le bouton « Faire Migrer »**

Le disque dur contenant les fichiers .cge doit avoir assez d'espace libre pour pouvoir contenir

une copie du fichier le plus volumineux de la liste. Selon le volume des données cryptées, il se peut que ce processus prenne un certain temps.

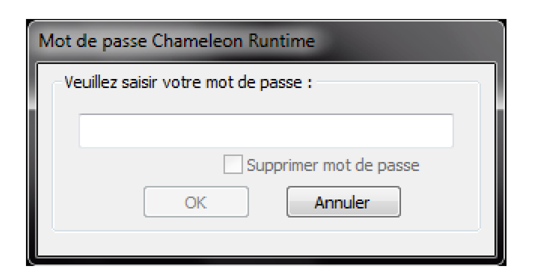
Vos disques cryptés seront rattachés une fois le processus de migration terminé.

Une fois le processus de migration terminé, seul le dispositif attaché pourra décrypter directement le fichier .cge. S’il s’agit d’un fichier que l’on avait fait migrer à partir d’un utilisateur retiré, alors l’utilisateur retiré n’aura plus accès à ce fichier.

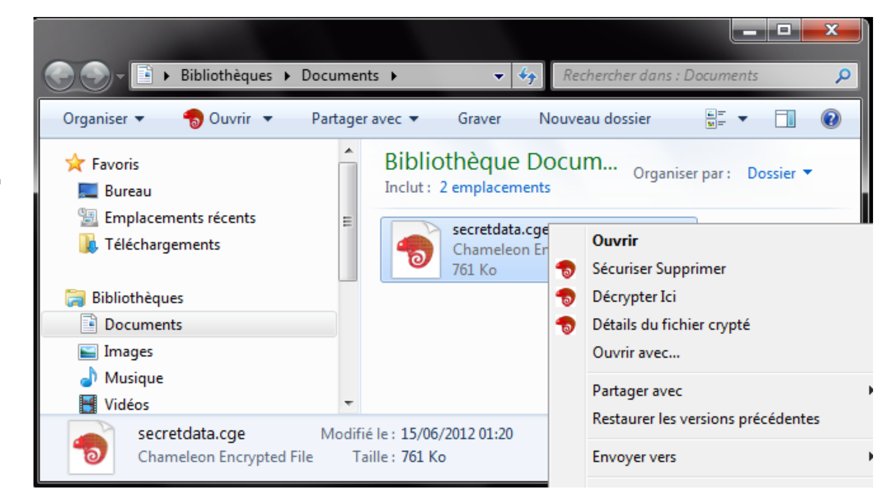
## 7.4 Voir les détails d’un fichier crypté

Pour voir les détails d’un fichier crypté :

1. **Connectez le dispositif**
2. **Saisissez votre mot de passe**




3. **Faites un clic droit sur le fichier .cge**
4. **Sélectionnez « Détails du Fichier Crypté »**

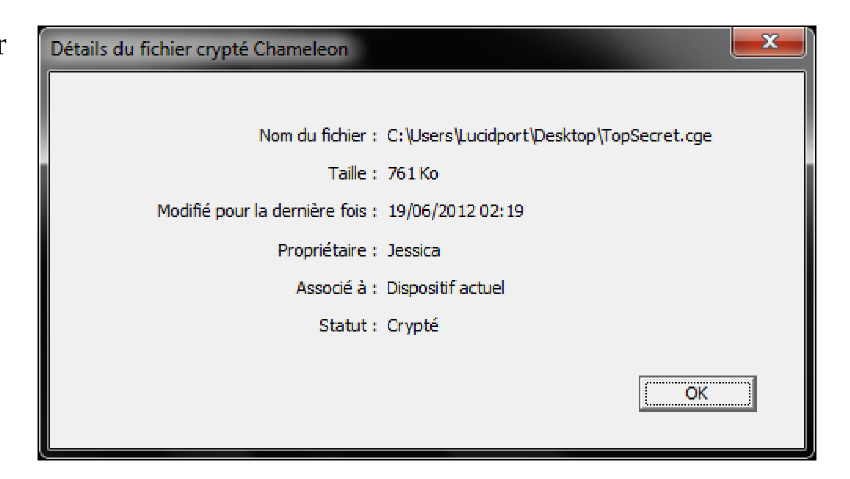






485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

5. Les détails du fichier s'affichent dans une nouvelle fenêtre



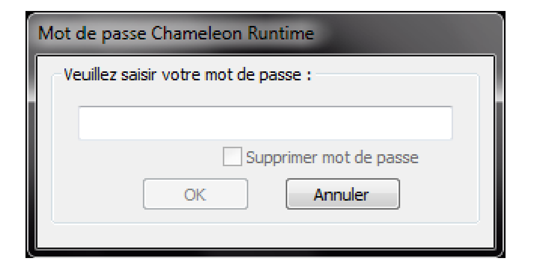

# 8 Changer de mot de passe

Bien qu'en option pour les dispositifs Utilisateur, la protection par mot de passe est toujours activée sur les dispositifs Master. La protection par mot de passe empêche toute utilisation non autorisée de votre dispositif Master. Un mot de passe doit être saisi à chaque fois que le dispositif est connecté, que l'ordinateur redémarre ou qu'il sort du mode veille.

Pour changer le mot de passe:

1. **Connectez le dispositif Master**

2. **Saisissez votre mot de passe**




3. **Démarrez le Gestionnaire Chameleon**

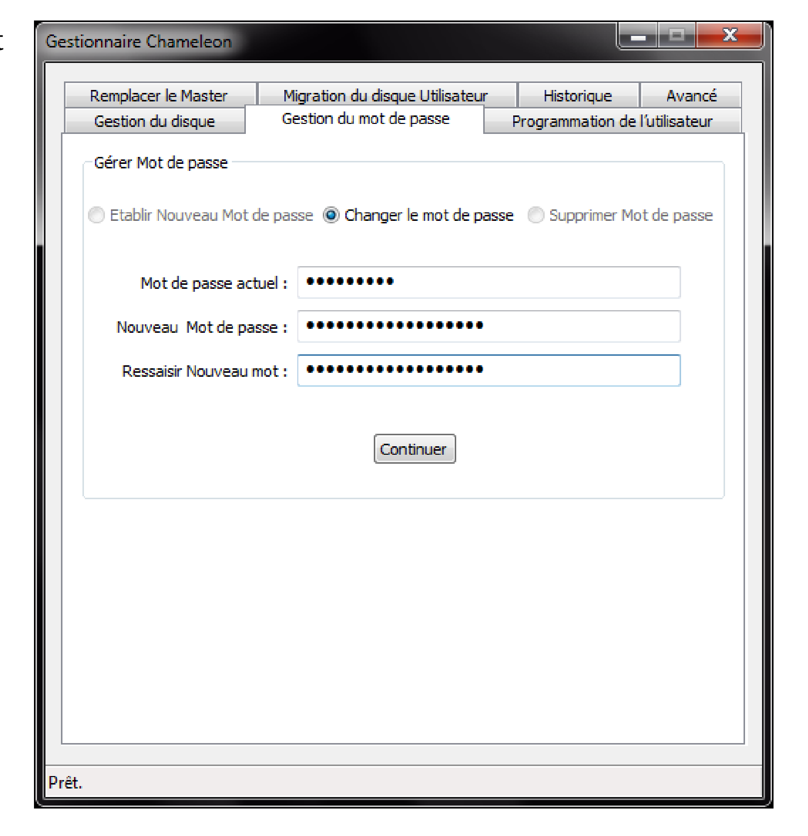
   Cliquez sur « Démarrer » de Windows >
   Tous les programmes >
   Chameleon >
   Gestionnaire Chameleon

4. **Sélectionnez l'onglet « Gérer Mot de Passe ».**

5. **Saisissez votre mot de passe existant**

6. **Saisissez le nouveau mot de passe et vérifiez-le.**

7. **Cliquez sur le bouton « Continuer ».**




Vous pouvez changer de mot de passe aussi souvent que vous le souhaitez. Il est possible d'avoir des doubles de dispositifs avec des mots de passe différents. Les dispositifs Master avec des mots de passe différents mais la même phrase de passe de récupération peuvent accéder aux mêmes données.

Si le mot de passe est oublié, le dispositif Master ne peut pas être déverrouillé; par contre, un double du Master peut être créé en utilisant la phrase de passe de récupération.

# 9 Ajouter, supprimer et modifier la taille des disques cryptés

Vous pouvez ajouter, supprimer ou modifier la taille des disques cryptés à n'importe quel moment. Le nombre de disques cryptés est limité par l'espace libre sur le disque et le nombre de lettres de volume disponibles. Les disques cryptés peuvent être créés sur votre disque dur interne mais également sur vos disques USB externes.

Pour gérer les disques cryptés:

1. **Connectez votre dispositif Master.**

2. **Démarrez le Gestionnaire Chameleon** — Cliquez sur « Démarrer » de Windows >
   Tous les programmes >
   Chameleon >



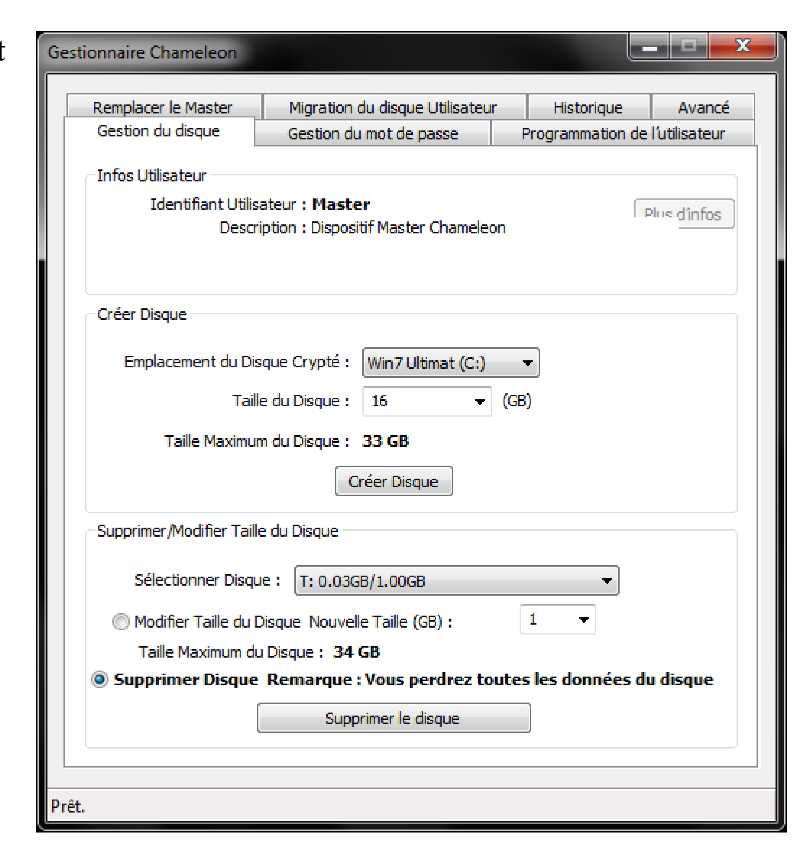




485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

Gestionnaire Chameleon

3. **Sélectionnez l'onglet « Gérer Disque ».**




- Pour ajouter un disque, indiquez la taille et l'emplacement du disque crypté, puis cliquez sur le bouton « Créer Disque ».

- Afin de supprimer un disque, sélectionnez le disque existant à partir du menu déroulant, puis sélectionnez « Supprimer Disque ». Cliquez sur le bouton « Supprimer Disque ». Il vous sera demandé de saisir une confirmation.

- Afin de modifier la taille d'un disque, sélectionnez votre disque à partir du menu déroulant, puis sélectionnez « Modifier Taille du Disque ». Saisissez la taille de votre choix, puis cliquez sur le bouton « Modifier Taille du Disque ». Lorsque vous réduisez la taille du disque, votre disque dur (C:\) doit avoir assez d'espace libre pour stocker temporairement le contenu entier du disque crypté.

# 10 Verrouillage PC (PC Lock)

En débranchant le dispositif Chameleon, vos données confidentielles sont protégées, mais les documents ouverts, les connexions réseau et les e-mails peuvent rester vulnérables. Le PC Lock verrouille automatiquement la session Windows à chaque fois que vous retirez le dispositif.

Pour activer le PC Lock sur le dispositif Master:



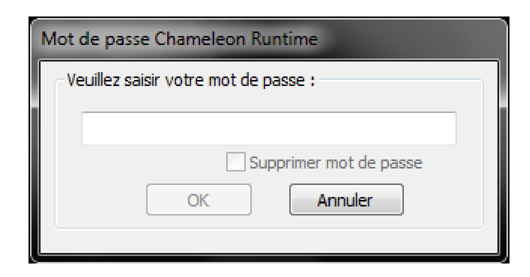




485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

1. **Connectez le dispositif Master**

2. **Saisissez le mot de passe**



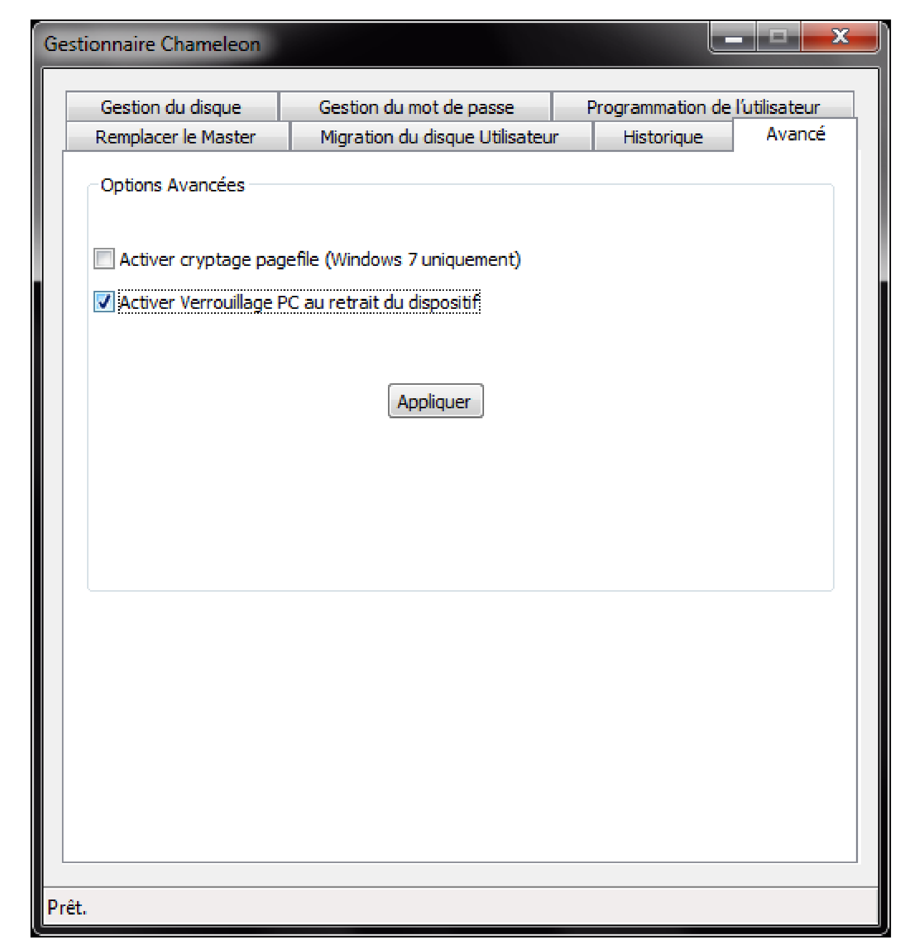

3. **Démarrez le Gestionnaire Chameleon**

   Cliquez sur « Démarrer » de Windows >
   Tous les programmes >
   Chameleon >
   Gestionnaire Chameleon

4. **Sélectionnez l'onglet « Avancé »**

5. **Sélectionnez « Activer PC Lock au retrait du dispositif »**

6. **Cliquez sur « Appliquer ».**

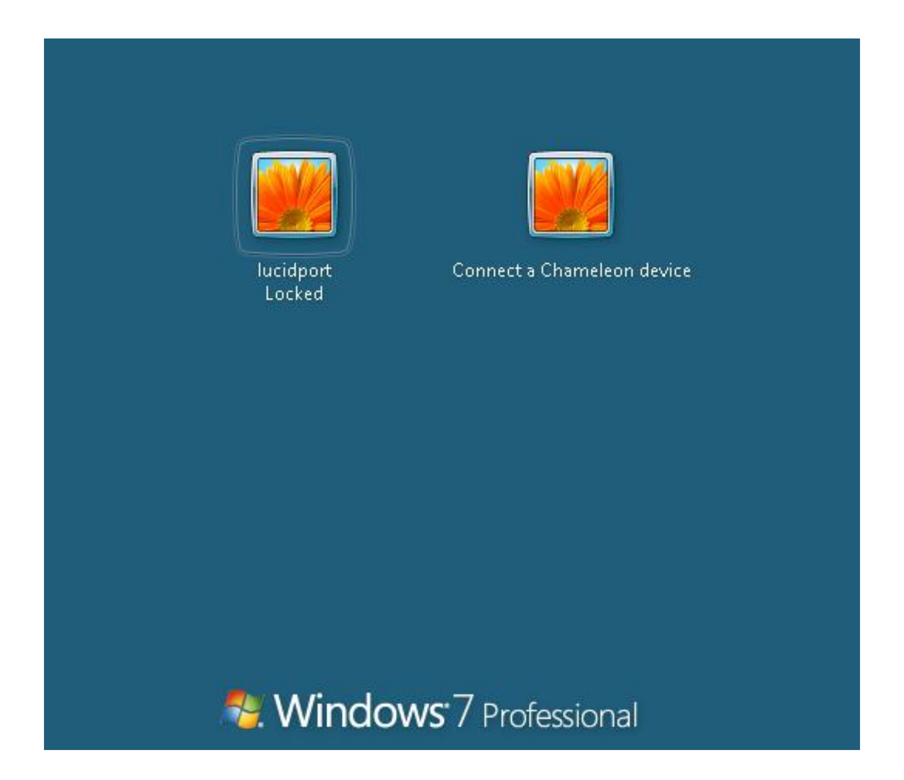



Lors de la programmation d'un dispositif Utilisateur, un Master a la possibilité d'imposer à ses Utilisateurs l'utilisation de PC Lock.

# 11 Connexion Automatique (AutoLogin)

L’Autologin Chameleon est le contraire de PC Lock : une fois activé, vous pouvez ouvrir une session Windows tout simplement en branchant le dispositif Chameleon. L’AutoLogin ne fonctionne que sous Windows Vista and Windows 7.

Lors de l’installation du logiciel Chameleon, un message (« Veuillez connecter votre dispositif ») s’ajoute à l’écran d’ouverture de session Windows, comme sur l’image ci-dessous.




Si l’AutoLogin n’avait pas été paramétré auparavant, l’écran d’ouverture de session vous demandera de saisir vos informations d’ouverture de session Windows.



485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com




Les informations d'ouverture de session seront vérifiées par le système d'exploitation. Si la connexion aboutit, les informations d'ouverture de session seront cryptées et sauvegardées. La prochaine fois que le dispositif sera connecté alors que l'écran de connexion est affiché, l'ouverture de session Windows se fera automatiquement.

L'Autologin ne fonctionne pas sur des dispositifs ayant un mot de passe activé. Puisque le mot de passe est obligatoire pour les Masters, l'Autologin ne fonctionne sur les dispositifs Master.

Les Masters ont la possibilité d'interdire leurs Utilisateurs d'utiliser l'AutoLogin.

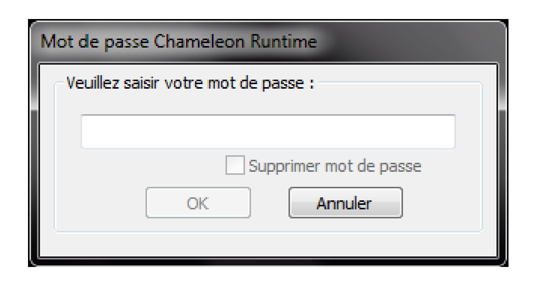
# 12 Fonctions supplémentaires et restrictions

## *12.1 Afficher la programmation d'un dispositif Utilisateur*

Pour vérifier la programmation d'un dispositif Utilisateur :

1. **Connectez le dispositif Utilisateur.**

2. **Saisissez le mot de passe**

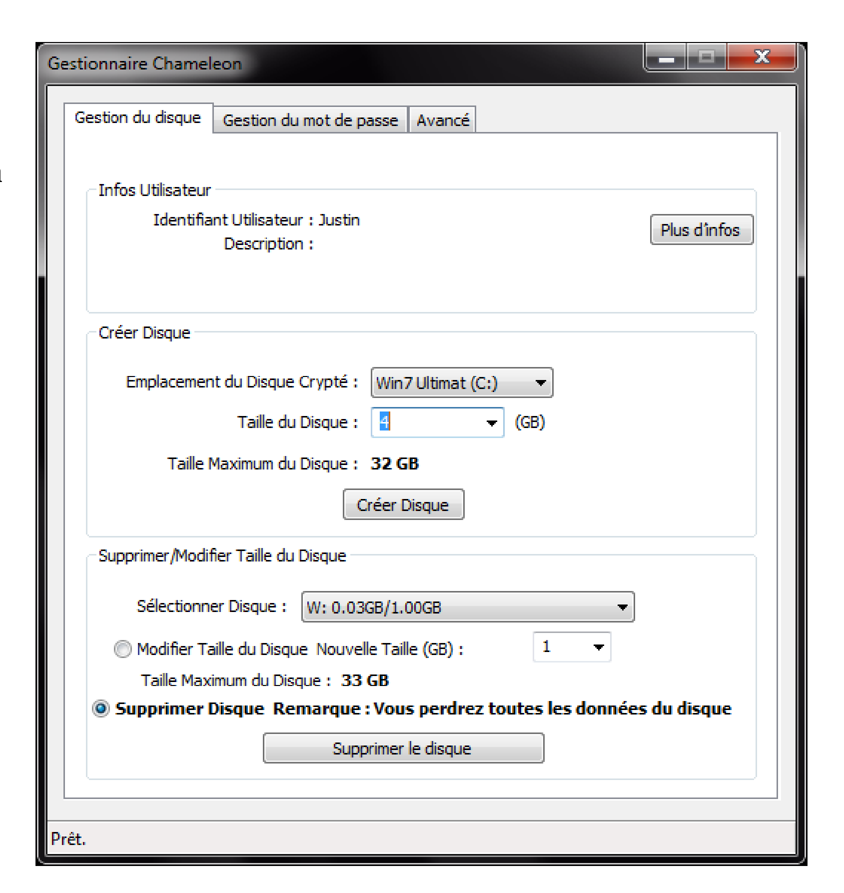



3. **Démarrez le Gestionnaire Chameleon**

Cliquez sur « Démarrer » de Windows >
Tous les programmes >
Chameleon >
Gestionnaire Chameleon

4. **Sélectionnez l'onglet « Gérer Disque ».**

5. **Cliquez sur le bouton « Plus d'info »**



6. La fenêtre Plus d'Info montre la configuration de l'Utilisateur.



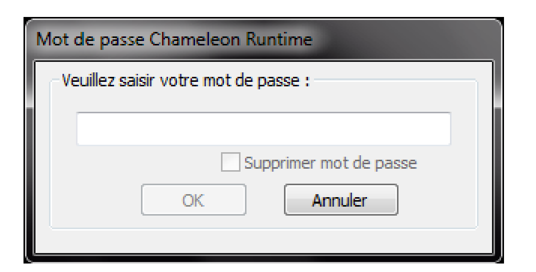

## 12.2 Fichier Windows de Pagination

Windows peut stocker des données temporaires dans son fichier de pagination (mémoire virtuelle). Ce fichier est généralement non crypté et est réactualisé continuellement. Activez le cryptage pagefile pour indiquer à Windows de crypter son fichier de pagination. Par défaut, le logiciel Chameleon ne crypte pas le fichier de pagination.

Pour activer le cryptage pagefile :

1. **Connectez le dispositif Chameleon.**

2. **Saisissez le mot de passe**

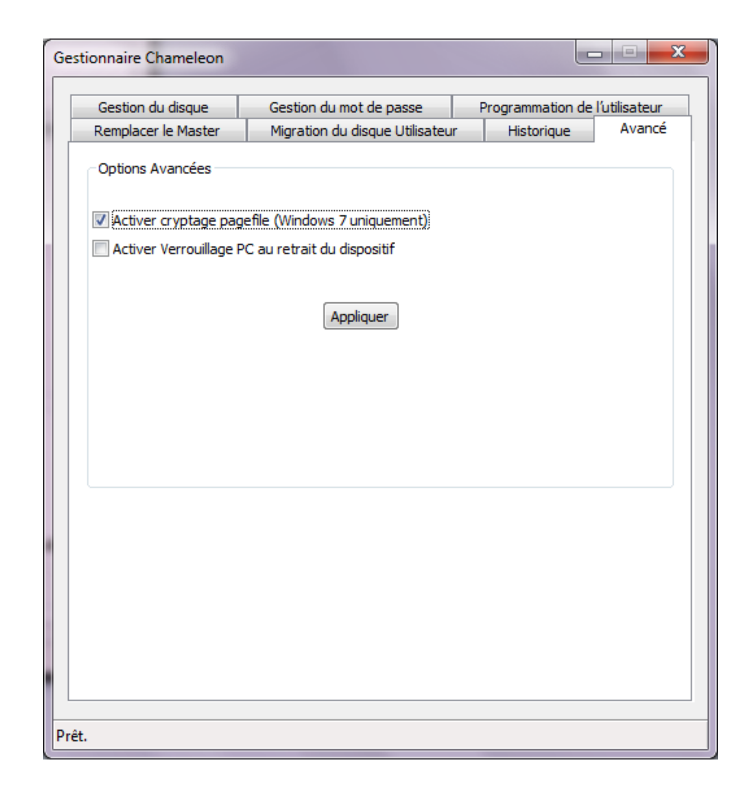



3. **Démarrez le Gestionnaire Chameleon**

   Cliquez sur « Démarrer » de Windows >
   Tous les programmes >
   Chameleon >
   Gestionnaire Chameleon

4. **Sélectionnez l'onglet « Avancé »**

5. **Sélectionnez « Activer Cryptage Pagefile »** puis **cliquez sur « Appliquer »**




Le cryptage du fichier de pagination élimine toute faille de sécurité potentielle, mais ralentit légèrement l'ordinateur. Seul Windows 7 permet le cryptage page file (ignoré pour les autres systèmes d'exploitation).

## *12.3 Retirer le dispositif de façon sécurisée*

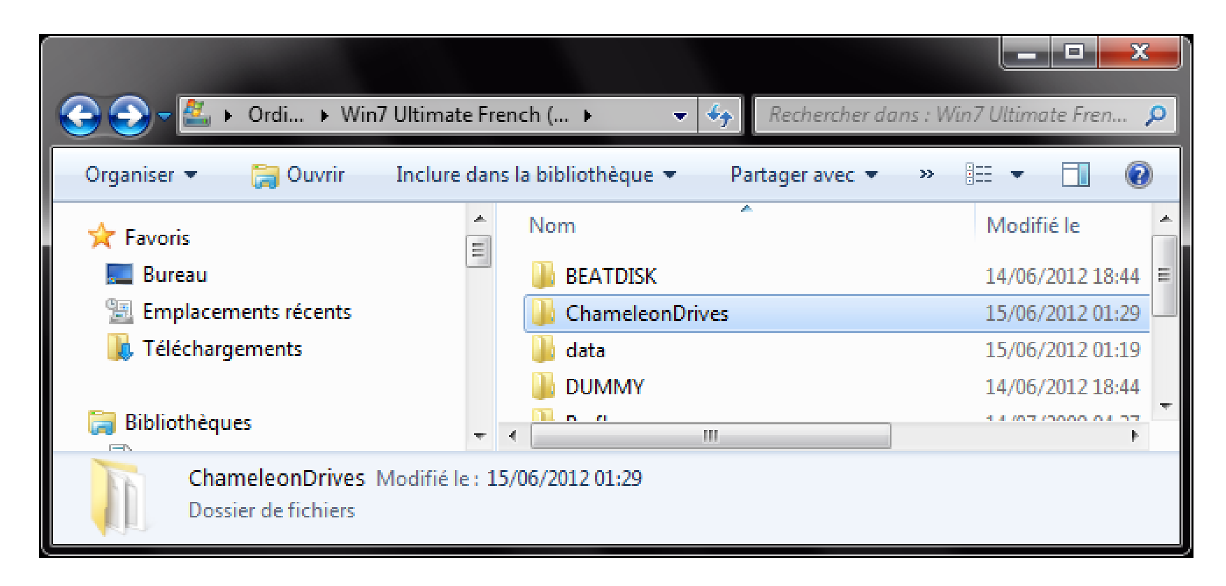
Un débranchement du dispositif alors que des données sont en cours d'écriture au disque crypté peut entraîner la corruption de ces données. Cette situation serait similaire à la déconnexion d'un disque dur externe alors qu'il serait en cours d'écriture. Afin d'être absolument certain qu'il n'y ait pas d'écriture en cours, utilisez la fonction « Retirer le périphérique en toute sécurité » de Windows avant de déconnecter le dispositif.




## *12.4 Créer des copies de sauvegarde des données*

Pour créer des copies de sauvegarde des disques cryptés, copiez le répertoire ChameleonDrives dans un autre emplacement. Ce répertoire se trouve dans le haut niveau de votre disque dur (par

ex : C:\ChameleonDrives\). Puisque les disques cryptés sont toujours cryptés, les copies de sauvegarde restent protégées. Il ne faut pas connecter le dispositif Chameleon pendant la création de copies de sauvegarde de vos données.




Vous pouvez ajouter le répertoire ChameleonDrives à la liste des copies de sauvegarde prévues.

AVERTISSEMENT : Ne copiez pas la sauvegarde du répertoire ChameleonDrives sur le haut niveau (racine) d'un disque (par ex : D:\ChameleonDrives). Le logiciel Chameleon n'est pas capable de distinguer l'original de sa copie. Si des disques identiques sont détectés dans le haut niveau, le logiciel Chameleon n'activera aucun des disques. Tous les sous-répertoires et emplacements réseau fonctionneront (par ex : D:\backup\ChameleonDrives).

### *12.5 Utilisation de plusieurs dispositifs Chameleon sur le même ordinateur*

Vous pouvez avoir plusieurs disques cryptés associés à des dispositifs Chameleon différents sur le même ordinateur.

Dans le cas où vous ne souhaiteriez plus utiliser un certain dispositif Chameleon sur un PC en particulier, supprimez son disque crypté à partir du Gestionnaire Chameleon, plutôt que de désinstaller le logiciel Chameleon. En désinstallant le logiciel Chameleon vous ne supprimez pas les disques cryptés.

Sauf pour la programmation de dispositifs Utilisateur, ne pas insérer plus d'un dispositif à la fois dans le PC.

## 13 Garantie limitée et Mentions Légales

Chameleon
Copyright (c) 2011, LucidPort Technology, Inc.





485 E. Evelyn Ave
Sunnyvale, CA 94086
USA
Tél: (001) 408 720 8800
Fax: (001) 408 720 8900

Veuillez contacter support@marathon6.com pour toute question technique.
Contactez sales@marathon6.com pour des renseignements concernant les ventes ou la garantie.
Visitez http://www.marathon6.com/chameleon pour les dernières mises à jour.

LucidPort Technology, Inc. garantit son produit contre tout défaut de matériel ou de fabrication dans des conditions normales d'utilisation et d'entretien pendant une période de un (1) année à partir de la date d'achat. La seule obligation de LucidPort Technology, Inc. relativement aux réclamations de non-conformité pendant la période de garantie décrite plus haut sera, à sa discrétion, de réparer ou de remplacer tout article de les produits.

Les obligations de garantie de LucidPort Technology, Inc. aux termes de la présente section dépendent expressément du respect des conditions qui suivent : (i.) les produits doivent être installés, utilisés et entretenus correctement en tout temps par le client; (ii.) les produits ne doivent pas être soumis à des contraintes mécaniques inhabituelles ou à des conditions environnementales ou électriques inhabituelles ou à d'autres forces majeures; (iii.) les produits ne doivent pas être soumis à une mauvaise utilisation, à un accident ou à une installation/désinstallation non autorisée par le client ou par un tiers; (iv.) les produits ne doivent pas être modifiés ou altérés d'une manière non autorisée, sauf approbation écrite ou intervention de LucidPort Technology, Inc. ; et (v.) le client doit installer rapidement toutes les mises à jour de produits publiées pour ces produits par LucidPort Technology, Inc. pendant la durée de la garantie. LucidPort Technology, Inc. ne garantit pas que les produits fonctionneront dans toute combinaison d'utilisation spécifique qui pourrait être choisie par le client ni que les produits fonctionneront sans interruption ou sans erreur ni que tous les défauts ou non-conformités seront corrigés. En outre, LucidPort Technology, Inc. n'aura aucune obligation de garantie pour toute défaillance de produits qui ne se conforment pas aux spécifications de produits applicables découlant de la combinaison d'un produit avec un matériel et/ou un logiciel non fourni par LucidPort Technology, Inc.

LucidPort Technology, Inc. décline toute responsabilité pour tout dommage ou toute perte de programmes, données ou autres renseignements sauvegardés sur tout support dans le matériel LucidPort Technology, Inc. ou tout produit extérieur à LucidPort Technology, Inc. ou toute pièce non couverte par la présente garantie. La récupération ou la réinstallation des programmes, données ou autres renseignements n'est pas couverte aux termes de la présente garantie limitée.

LucidPort Technology, Inc. décline toute responsabilité dans le cas d'une vente non autorisée ou




d'une représentation trompeuse par des tiers revendeurs non autorisés. Les garanties LucidPort Technology, Inc. ne sont pas cessibles avec la propriété. Les produits achetés lors d'encans, ventes-débarras, marchés aux puces ou à titre d'appareils de démonstration peuvent ne pas être couverts aux termes de la présente garantie LucidPort Technology, Inc.

LUCIDPORT TECHNOLOGY, INC. DÉCLINE TOUTE RESPONSABILITÉ EN CAS DE DOMMAGES DIRECTS, SPÉCIAUX, INDIRECTS OU CONSÉCUTIFS DÉCOULANT D'UNE RUPTURE DE GARANTIE OU DE CONDITION, Y COMPRIS LES FRAIS DE RÉCUPÉRATION OU DE REPRODUCTION DE TOUT PROGRAMME OU DE TOUTES DONNÉES STOCKÉS DANS OU UTILISÉS AVEC LE PRODUIT LUCIDPORT TECHNOLOGY, INC. LUCIDPORT TECHNOLOGY, INC. NE FAIT PAS SPÉCIFIQUEMENT VALOIR QU'ELLE POURRA RÉPARER TOUT PRODUIT AUX TERMES DE LA PRÉSENTE GARANTIE LIMITÉE OU ÉCHANGER LE PRODUIT SANS RISQUE OU PERTE DE PROGRAMMES OU DE DONNÉES.

The AES encryption technology in the Chameleon is classified by the United States government as an ECCN 5A002 item and can be exported under License Exception ENC, Sec. 740.17 (b)(3) of the Export Administration Regulations ("EAR"). The Chameleon may not be used or otherwise exported or re-exported into (or to a national or resident of) Cuba, Iran, North Korea, Sudan, or Syria. No further approvals or authorizations from the US government are required.




485 E. Evelyn Ave., Sunnyvale, CA 94086 / Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com